

10/527992

Rec'd PCT/PTO 21 MAR 2005

020638 PCT
PCT/JP03/12022

日本国特許
JAPAN PATENT OFFICE

REC'D 10 OCT 2003
WIPO PCT
19.09.03

#2

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:

2002年 9月20日

出願番号
Application Number:

特願2002-276306

[ST.10/C]:

[JP2002-276306]

出願人
Applicant(s):

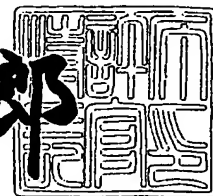
パイオニア株式会社

PRIORITY
DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2003年 6月26日

特許庁長官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3050540

Best Available Copy

【書類名】 特許願

【整理番号】 57P0255

【提出日】 平成14年 9月20日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/08
H04L 9/14

【発明者】

【住所又は居所】 埼玉県所沢市花園4丁目2610番地 パイオニア株式会社 所沢工場内

【氏名】 竹村 到

【発明者】

【住所又は居所】 埼玉県所沢市花園4丁目2610番地 パイオニア株式会社 所沢工場内

【氏名】 吉田 和幸

【特許出願人】

【識別番号】 000005016

【氏名又は名称】 パイオニア株式会社

【代理人】

【識別番号】 100107331

【弁理士】

【氏名又は名称】 中村 聡延

【電話番号】 03-5524-2323

【選任した代理人】

【識別番号】 100104765

【弁理士】

【氏名又は名称】 江上 達夫

【電話番号】 03-5524-2323

【手数料の表示】

【予納台帳番号】 131957

特2002-276306

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0104687

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 鍵管理システム

【特許請求の範囲】

【請求項 1】 複数の情報受信者をリーフに割り当てた木構造を規定する手段と、

前記木構造を所定階層毎に分割して複数の部分木を規定する手段と、

前記複数の部分木の各部分木に対して鍵情報の割り当てを行う手段と、
を有することを特徴とする鍵管理システム。

【請求項 2】

前記鍵情報の割り当てを行う手段は、

前記部分木のリーフに割り当てられた複数の情報受信者全てにより構成される集合と、前記部分木中の特定のノード以下のリーフに割り当てられた情報受信者との差分集合を、前記部分木中の全てのノードについて特定する手段と、

前記差分集合の各々に鍵情報を割り当てる手段と、

前記複数の情報受信者の各々に対して、当該情報受信者が属する全ての差分集合に割り当てられた鍵情報を割り当てる手段と、

からなることを特徴とする請求項 1 記載の鍵管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、木構造を用い、特定の受信者の無効化機能を有する鍵管理方式に関する。

【0002】

【従来の技術】

映画、音楽などの著作物であるコンテンツの著作権を保護するために、情報を利用してコンテンツを暗号化して提供することが行われている。そのようなシステムの一例では、再生装置には複数のデバイス鍵を与え、記録媒体には暗号化されたコンテンツと、再生を許可された再生装置のみがコンテンツの復号鍵を生成できるようにした鍵生成情報とを記録する。再生を許可された再生装置は、鍵生

成情報からコンテンツの復号鍵を生成し、その復号鍵を使用してコンテンツを復号して再生する。一方、再生を許可されていない（無効化された）再生装置は、コンテンツの復号鍵を生成できないので、暗号化されているコンテンツを再生することはできない。

【0003】

このようなシステムで、鍵情報を管理するための手法として木構造を用いた鍵管理方式が提案されており、その例として「The Complete Subtree Method」、
「The Subset Difference Method」などが知られている（例えば非特許文献1参照。）。これらの方式では、コンテンツの復号鍵を生成するための鍵生成情報が不正に暴露されたり漏洩した場合には、その鍵生成情報を無効化するための処理が可能となっている。

【0004】

また、上記のような方式に基づいてデジタルコンテンツの保護を行う方法も提案されている（例えば非特許文献2参照。）。

【0005】

【非特許文献1】

Dalit Naor, Noni Naor, and Heff Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers", Lecture Notes in Computer Science, Vol.2139, pp.41-62, 2001

【非特許文献2】

中野稔久、他3名、"デジタルコンテンツ保護用鍵管理方式—木構造パターン分割方式—"、2002年暗号と情報セキュリティシンポジウム講演論文集、2002年2月1日

【0006】

【発明が解決しようとする課題】

上述のThe Subset Difference Methodにおいては、受信者は自分の属する全ての差分集合に割り当てられた鍵を保有しておかなければならないため、受信者側に多くの記憶容量を必要とする。疑似乱数生成器を用いることでこの情報量を削減することはできるのであるが、それでもThe Complete Subtree Methodと比較

すると10倍以上の情報記憶容量が要求される。一方、The Complete Subtree Methodについては、受信者側に記憶すべき情報量は少ないが、受信者へ伝送される（情報の伝送に記録媒体を利用する場合には、記録媒体に記録される）鍵情報量が大きくなりすぎてしまう。本発明が解決しようとする課題には、上記のものが一例として挙げられる。

【0007】

【課題を解決するための手段】

請求項1に記載の発明は、鍵管理システムにおいて、複数の情報受信者をリーフに割り当てた木構造を規定する手段と、前記木構造を所定階層毎に分割して複数の部分木を規定する手段と、前記複数の部分木の各部分木に対して鍵情報の割り当てを行う手段と、を有することを特徴とする。

【0008】

【発明の実施の形態】

以下、図面を参照して本発明の好適な実施の形態について説明する。まず、鍵管理方式について基礎的な説明を行い、続いて本発明の方式を説明する。

【0009】

(1.1) 受信者の無効化機能を有する鍵管理方式

送信者が多数の受信者に対して同一の情報を伝送するシステムにおいて、信頼できる鍵管理機関が、あらかじめ全ての受信者に伝送情報を復号するための秘密情報を配布しておき、その秘密情報を持たない受信者が送信者からの情報を復号できないように、送信者側で情報を暗号化して伝送する方法がある。この場合に問題となるのは、全ての受信者が同一の秘密情報を保有している場合、悪意ある受信者が自分の保有する秘密情報を1回公開してしまえば、その後に伝送される情報は誰にでも復号が可能になってしまうことである。

【0010】

この問題の対策として、鍵管理機関が受信者毎に異なる秘密情報を配布し、特定の受信者の秘密情報が漏洩した場合、その受信者の保有していた秘密情報を用いても伝送された情報を復号できないようにする手法、即ち、受信者の無効化機能を有する鍵管理方式がある。本発明はそのような鍵管理方式を扱う。

【0011】

ここでは、情報の伝送は特定の送信者から多数の受信者への片方向伝送のみであり、また受信者に最初に秘密情報（復号鍵等）を割り当てる以外は、受信者の保有する秘密情報を一切変更できないようなアプリケーションを想定している。

【0012】

受信者の無効化機能を有する鍵管理方式を適用した情報配信システムの1つのモデルを図1（a）に示す。図示のように、情報配信システムは、鍵管理機関1、情報送信者2及び情報受信者3の3つの要素から構成される。以下、各要素について説明する。

【0013】

・鍵管理機関

鍵管理機関1は、情報送信者2が伝送する伝送情報6（暗号文）を復号するための秘密情報（暗号文復号用鍵4aなど）を各受信者に割り当てる。また、鍵管理機関1は、伝送情報6を復号不可能にしたい受信者（今後、ある特定の受信者に対して、伝送される情報を復号できないようにすることを「受信者の無効化」と呼ぶ）の集合から、前記集合以外の受信者のみが復号できるような鍵情報4bを生成し、伝送情報6を暗号化するための鍵（暗号化用鍵情報5）とあわせて情報送信者への配送も行う。

【0014】

ここで各受信者に割り当てる秘密情報（復号用鍵4aなど）と伝送情報6の暗号化に用いられる鍵（暗号化用鍵情報5）の生成・保管・配送は安全に行われるものと仮定する。

【0015】

・情報送信者

情報送信者2は、鍵管理機関1から配送された、伝送情報の暗号化用鍵情報5を用いて伝送情報6を暗号化し、無効化されていない受信者のみが復号できる鍵情報4bと一緒に伝送情報6（暗号文）を受信者に伝送する。

【0016】

・情報受信者

無効化されていない受信者については、伝送情報 6 (暗号文) を受信したとき、受信者が持つ秘密情報 (暗号文復号用の鍵 4 a 等) を使って受信した鍵情報 4 b を復号し、復号された鍵を用いて暗号文から伝送情報 6 を復号する。逆に無効化されている受信者については、そのような受信者が複数結託しても、伝送情報に関して何の情報も得られない。また、ここでは多数の受信者の存在を想定している。

【0017】

以下、上記構成要素について詳しく説明する。

【0018】

\underline{N} を全ての受信者の集合とし、その要素数を $|\underline{N}| = N$ とする。 \underline{N} の部分集合 \underline{R} を無効化したい受信者の集合とし、その要素数を $|\underline{R}| = r$ とする。受信者の無効化機能を有する鍵管理方式の目的は、鍵管理機関 (又は情報送信者) が受信を許可した受信者、つまり \underline{R} に含まれない全ての受信者 $u \in \underline{N} \setminus \underline{R}$ が伝送される情報を復号でき、逆に受信を許可されていない \underline{R} に含まれる受信者全てが結託しても全く伝送情報を得られないようにすることである。

【0019】

(a) 鍵管理機関

(i) 初期設定

受信者全体の集合 \underline{N} の部分集合 $\underline{S}_1, \underline{S}_2, \dots, \underline{S}_w$ ($\forall j, \underline{S}_j \subseteq \underline{N}$) を定義する。各 \underline{S}_j には暗号 (復号) 鍵 L_j が割り当てられる。ここで各 L_j は一様に分布しており、互いに独立な値を割り当てるのが望ましい。各受信者 (受信装置) u には、秘密情報 I_u を割り当てる。ここで \underline{S}_j に含まれる全ての受信者 $u \in \underline{S}_j$ が、自分に割り当てられた秘密情報 I_u から、自分の属する部分集合 \underline{S}_j に割り当てられた復号鍵 L_j を求められるように秘密情報 I_u を割り当てなければならない。また、 \underline{S}_j に含まれない全ての受信者 $u \in \underline{N} \setminus \underline{S}_j$ が結託しても復号鍵 L_j を求めることができないように秘密情報 I_u を割り当てなければならない。

【0020】

(ii) 鍵情報生成

(1) 伝送情報 M の暗号化、復号化に用いる鍵 (セッション鍵) K を選ぶ。

【0021】

(2)無効化する受信者の集合 \underline{R} の補集合 $\underline{N} \setminus \underline{R}$ に属する受信者 $u \in \underline{N} \setminus \underline{R}$ をいくつかの部分集合 \underline{S}_{i1} 、 \underline{S}_{i2} 、 \dots 、 \underline{S}_{im} に分割する。

【0022】

【数1】

$$\underline{N} \setminus \underline{R} = \bigcup_{j=1}^m \underline{S}_{ij} \quad (1-1)$$

【0023】

ここで、初期設定で上記部分集合に割り当てられてた暗号鍵をそれぞれ L_{i1} 、 L_{i2} 、 \dots 、 L_{im} とする。

【0024】

(3)暗号鍵 L_{i1} 、 L_{i2} 、 \dots 、 L_{im} を用いてセッション鍵 K を m 回暗号化して式(1-2)を生成、セッション鍵 K と一緒に情報送信者に配送する。

【0025】

【数2】

$$(i_1, i_2, \dots, i_m, E_{enc}(K, L_{i1}), E_{enc}(K, L_{i2}), \dots, E_{enc}(K, L_{im})) \quad (1-2)$$

【0026】

ここで、情報送信者へのセッション鍵の配送は安全に行われるものと仮定する。また、 E_{enc} は暗号化アルゴリズムである。本システムで用いられる暗号、復号化アルゴリズムは2種類あり、以下にまとめる(ただし、2つのアルゴリズムに全く同じものを使用しても構わない)。

【0027】

・ 伝送情報 M の暗号化アルゴリズム F_{enc} 、復号化アルゴリズム F_{dec}

セッション鍵 K を用いて暗号文 $C_K = F_{enc}(M, K)$ を生成する。高速性が要求される。

【0028】

・セッション鍵暗号化アルゴリズム E_{enc} 、復号化アルゴリズム E_{dec}
セッション鍵の配送に用いる。 F_{enc} よりも暗号化アルゴリズムの安全性が
要求される。

【0029】

(b) 情報送信者

セッション鍵 K と特定の受信者のみが復号できる鍵情報を鍵管理機関から受け
取り、セッション鍵 K を鍵として暗号化アルゴリズム F_{enc} を用いて伝送情報 M
を暗号化して、暗号文

【0030】

【数3】

$$\langle [i_1, i_2, \dots, i_m, E_{enc}(K, L_{i_1}), E_{enc}(K, L_{i_2}), \dots, E_{enc}(K, L_{i_m})], F_{enc}(M, K) \rangle \quad (1-3)$$

【0031】

を伝送する。なお、式 (1-3) の [] 内の部分を $F_{enc}(M, K)$ のヘッダーと
呼ぶことにする。

【0032】

(c) 情報受信者

受信者 u は、情報送信者により暗号化された次の暗号文を受信する。

【0033】

【数4】

$$\langle [i_1, i_2, \dots, i_m, C_1, C_2, \dots, C_m], C_K \rangle \quad (1-4)$$

【0034】

- (1) $u \in S_{ij}$ であるような i_j を探索する。($u \in R$ の場合、存在しない。)
- (2) 自身の保有する秘密情報 I_u から L_{ij} を求める。

【0035】

- (3) $K = E_{dec}(C_j, L_{ij})$ を求める。

【0036】

(4) $M = F_{\text{dec}}(C_K, K)$ を求める。

【0037】

上記鍵管理方式を実現するアルゴリズムとして以下の方式がある。

- ・ The Logical Key Hierarchy Method
- ・ CPRM Common Cryptographic Key Management
- ・ The Complete Subtree Method
- ・ The Subset Difference Method
- ・ Tree Pattern Division Method

上記方式の違いとしては、(1) 受信者の部分集合 S_1, \dots, S_w の定義、(2) 各部分集合に対する鍵の割り当て方法、(3) 受信を許可する（無効化しない）受信者の集合 $N \setminus R$ の分割方法、(4) 各受信者 u が行う自分の属する部分集合 S_j の探索方法と、 I_u から鍵 L_{S_j} の求め方等が挙げられる。

【0038】

各方式は以下の3つの観点から評価される。

【0039】

- ・ 伝送情報の量

暗号文 $F_{\text{enc}}(M, K)$ に付加されるヘッダー量。一般に $N \setminus R$ を分割した部分集合の数 m に比例する。

【0040】

- ・ 受信者が保有しておく秘密情報 I_u の量

復号用の鍵等の秘密情報を受信者がどれだけ保持しておかなければならないか。

【0041】

- ・ 受信者が伝送された情報を復号するのに要する演算量

(1.2) 基礎となる方法 (The Subset Difference Method)

(1.2.1) 部分集合 S_1, \dots, S_w の定義

最初に受信者全体の集合 N の部分集合 S_1, \dots, S_w を定義する。この部分集合に対して暗号（復号）鍵、又は復号鍵を導けるような情報 L_1, \dots, L_w を割り当てることになる。 N 枚のリーフを持つ2分木のリーフに各受信者を割り当て

る（ここで N は2の冪であるとしている。）。

【0042】

受信者の部分集合を次のように表す。2分木中の任意のノード v_i （ルートとリーフもノードに含まれる。）をルートとする部分木の全てのリーフに割り当てられた受信者の集合を \underline{S}_i で表す。任意のノード v_i 以下のリーフに割り当てられた受信者の集合 \underline{S}_i とノード v_i をルートとする部分木中の（ルートを除く）ノード v_j をルートとする部分木の全てのリーフに割り当てられた受信者の集合 $\underline{S}_j \subset \underline{S}_i$ について、 \underline{S}_i の要素から \underline{S}_j の要素を引いた差分集合を $\underline{S}_{i,j}$ とする。つまり、集合 \underline{S}_i に含まれる受信者のうち、集合 \underline{S}_j に含まれていない受信者の集合を $\underline{S}_{i,j}$ とする。図2は $\underline{S}_{i,j}$ を示している。この差分集合に対して1つの鍵 $L_{i,j}$ を割り当てる。

【0043】

(1.2.2) $\underline{N} \setminus \underline{R}$ の分割方法

次に受信を許可する（無効化しない）受信者の集合 $\underline{N} \setminus \underline{R}$ を、上記で定義された差分集合 $\underline{S}_{i1,j1}, \underline{S}_{i2,j2}, \dots, \underline{S}_{im,jm}$ に分割する方法を説明する。2分木のルートと無効化したい受信者に相当する各リーフを結ぶ最短のパス上のノードのみで構成される部分木 $ST(\underline{R})$ を考える（このような部分木は \underline{R} から一意に構成される）。 $ST(\underline{R})$ については子ノードの存在しないノードをリーフと呼ぶことにする。以下のアルゴリズムを $ST(\underline{R})$ がルートのノードのみになるまで繰り返し、 $\underline{N} \setminus \underline{R}$ を構成する差分集合を選択する。

【0044】

(1) 2つのリーフからルートへのパスの共通部分に存在するノードの中で、リーフとの距離が最小となるノードを2つのリーフの最小共通ノードと呼ぶことにする。 $ST(\underline{R})$ のリーフ v_i, v_j を、それらの最小共通ノード v 以下に他のリーフが存在しないように選ぶ。 v の2つの子ノードの中で、 v と v_i のパス上に存在する子ノードを v_k 、 v と v_j のパス上に存在する子ノードを v_l とする。（リーフが $ST(\underline{R})$ 中に1つしか存在しない場合、 $v_i = v_j$ 、 $v = v_l = v_k$ として、 v を $ST(\underline{R})$ のルートと考えればよい。）

(2) $v_k \neq v_l$ ならば、 $\underline{N} \setminus \underline{R}$ を構成する差分集合に $\underline{S}_{k,i}$ を加える。 $v_l \neq v_j$ な

らば $N \setminus R$ を構成する差分集合に $S_{1,j}$ を加える。

【0045】

(3) v より下に位置するノードを全て除去する。これにより v がリーフになる。

【0046】

上記アルゴリズムを用いることにより、受信者の集合 $N \setminus R$ は、無効化したい受信者数 $|R| = r$ のとき、最大 $2r - 1$ の差分集合に分割される。

【0047】

(1.2.3) 部分集合 S_1, \dots, S_w への鍵の割り当て方法

次に、各差分集合に対する鍵の割り当て方法について説明する。各差分集合に対して、一様に分布しており、互いに独立な値を持つ鍵を割り当てる。

【0048】

(1.2.4) 受信者への秘密情報の割り当て方法

各受信者には自分の属する差分集合全ての鍵を配布しておかなければならない。これは受信者側に非常に多くの記憶量を必要とする。受信者 u は、自分の属する各部分木 T_k に対して（ここで T_k の変数 k は部分木の高さを表している。）、部分木 T_k 中に存在するノードの中で、 T_k のルートから u のパス上に存在するものを除く全てのノードの数に相当する鍵を保有しなければならない。受信者 u の属する部分木の数は $\log_2 N$ 個存在し、各部分木の高さは $1 \leq k \leq \log_2 N$ であるから、受信者が保有しなければならない鍵の数は式 (2-1) のようになる。

【0049】

【数5】

$$1 + \sum_{k=1}^{\log_2 N} (2^{k+1} - k - 2) \quad (2-1)$$

【0050】

(1.2.5) 部分集合 S_1, \dots, S_w への鍵の割り当て方法（擬似乱数生成器を用いる場合）

受信者が保有しておく鍵を減らすため、各差分集合 $S_{i,j}$ に直接鍵を割り当て

るのではなく、部分集合 \underline{S}_i に対して1つのラベルを割り当て、差分集合 $\underline{S}_{i,j}$ ($\forall j, \underline{S}_j \subset \underline{S}_i$) に割り当てる鍵 $L_{i,j}$ が、部分集合 \underline{S}_i に割り当てられたラベルを用いて導けるようにしておく。このとき、差分集合 $\underline{S}_{i,j}$ 内に存在する受信者のみが鍵 $L_{i,j}$ を導けるようにしなければならない。以下では、擬似乱数生成器を用いて、上記方法を実現する方法を示す。

【0051】

$G: \{0, 1\}^n \rightarrow \{0, 1\}^{3n}$ を入力長の3倍の長さを出力する擬似乱数生成器とする。擬似乱数生成器 G の入力を S としたとき、出力される値を3等分した左側部分を $G_L(S)$ で表し、右側部分を $G_R(S)$ 、中央部分を $G_M(S)$ で表す。また、 G の入力として乱数を与えたときに出力される値と、出力と同じ長さの真の乱数を多項式時間の計算能力をもつ攻撃者に与えたとき、攻撃者は、有意な確率で両者を区別できないといった特性を G は満たしていなければならない。

【0052】

ノード v_i をルートとする部分木 T_i を考える。ノード v_i にラベル $LABEL_i$ を割り当てる（簡単のため任意の部分木のリーフに割り当てられた受信者の集合へのラベルの割り当てを、その部分木のルートノードにラベルを割り当てると表現する。つまり上記表現は次のようになる。「部分木 T_i 中のリーフに割り当てられた受信者の集合 \underline{S}_i にラベル $LABEL_i$ を割り当てる。」）。 $LABEL_{i,j}$ を、部分木 T_i 中のノード v_j のラベルとする（割り当てられるラベルが多変数のパラメータを持つ（この場合 i と j の2変数）場合、それは差分集合に対して割り当てられたラベルを示している。このとき、 $LABEL_{i,j}$ は v_j をルートとする部分木のリーフに割り当てられた受信者の集合 \underline{S}_j に割り当てられるのではなく、 \underline{S}_i に含まれ、 \underline{S}_j には含まれていない受信者の集合（差分集合） $\underline{S}_{i,j}$ に対して割り当てられる。）。 $LABEL_{i,j}$ が差分集合 $\underline{S}_{i,j}$ に割り当てられるラベルである。

【0053】

$LABEL_{i,j}$ を部分木 T_i のルート v_i に割り当てられたラベル $LABEL_i$ から擬似乱数生成器 G を用いて以下の導出規則により導く。ラベルを擬似乱数生成器の入力としたとき、その出力を次のように定義する。 G_L - 左側の子ノードのラベル、 G_R

一右側の子ノードのラベル、 G_M -入力ラベルの割り当てられたノードに割り当てる暗号（復号）鍵。この導出規則に拠れば、部分木 T_i 中のある親ノードにラベル S が割り当てられたとき、その2つの子ノードのラベルは、 $G_L(S)$ 、 $G_R(S)$ が割り当てられる。これより、 v_i から v_j に至るパス上のノードに割り当てるラベルを G を用いて順次求めることで、 v_i に割り当てられたラベル $LABEL_i$ から、部分木 T_i 中のノード v_j のラベル $LABEL_{i,j}$ を求めることができる。

【0054】

最後に $LABEL_{i,j}$ を G の入力としたときの出力の中央部分 $G_M(LABEL_{i,j})$ を、差分集合 $S_{i,j}$ に割り当てる暗号（復号）鍵 $L_{i,j}$ として用いる。図3（a）に部分木 T_i 中のノード v_j に割り当てるラベルと暗号（復号）鍵の生成方法を示す。

【0055】

このような方法を用いれば、部分木中のあるノードのラベルが与えられたとき、その子孫ノード全てのラベルと暗号（復号）鍵を計算することができる。逆に、あるノード v_j の先祖ノードのラベルを v_j から求めることはできない。さらに、ノード v_j の全ての子孫ノードのラベル（ただし、 v_j 自身のラベルは含まない）から暗号（復号）鍵 $L_{i,j}$ を求めることはできない。部分木 T_i のルートのラベル $LABEL_i$ を与えられたとき、差分集合 $S_{i,j}$ に割り当てられる暗号（復号）鍵 $L_{i,j}$ を計算するのに擬似乱数生成器 G を最大で $\log_2 N + 1$ 回用いる。

【0056】

(1.2.6) 受信者への秘密情報の割り当て方法（擬似乱数生成器を用いる場合）

各受信者 u が保有する秘密情報 I_u の割り当て方法について説明する。受信者 u は、自分の属する各部分木 T_i に対して、 T_i のルートノード v_i と、部分木 T_i 中のノードで u の先祖ノードでない全てのノード v_j により決定される差分集合 $S_{i,j}$ に割り当てられた暗号（復号）鍵 $L_{i,j}$ を計算できなければならない。部分木 T_i のルートノード v_i から u へのパスを考え、そのパスに直接ぶら下がるノードを v_{i1} 、 v_{i2} 、 \dots 、 v_{ik} とする（図2（b）参照）。つまり、それらはパスに隣接するノードの中で、 u の先祖ノードでないノードである。部分木 T_i 中で u の先祖でない任意のノード v_j は、これらのノード v_{i1} 、 v_{i2} 、 \dots 、 v_{ik}

いずれかの子孫ノードである。ゆえに、受信者 u が I_u として、 v_{i1} 、 v_{i2} 、
 \dots 、 v_{ik} に割り当てられたラベルを保有しておけば、最大 $\log_2 N + 1$ 回擬似乱数
 生成器 G を用いて、部分木 T_i 中でパス上に存在しない任意ノード v_{ij} に割り当
 てられた復号鍵 $L_{i,j}$ を計算することができる。

【0057】

受信者 u を含む高さ k の部分木 T_i 中に、受信者 u が保存しておかなければなら
 ないラベルは k 個あるから、これを u を含む各部分木について考えると、受信
 者 u があらかじめ保有しておかなければならない復号鍵（ラベル）の数は式（2-
 2）のようになる。

【0058】

【数6】

$$1 + \sum_{k=1}^{\log_2 N} k = 1 + \frac{(1 + \log_2 N) \log_2 N}{2} = \frac{1}{2} (\log_2 N)^2 + \frac{1}{2} \log_2 N + 1 \quad (2-2)$$

【0059】

式（2-2）で1が足されているのは、無効化する受信者が全く存在しない場合
 の鍵が必要だからである。

【0060】

（1.2.7）複数の2分木を用いる方法

さらに受信者 u が保有する秘密情報 I_u を減らす場合は、伝送情報 M の量との
 トレードオフとなる。一つの方法として、2分木を高さの低い木に限定して複数
 用いる方法がある。木構造においてノードの位置する各層をレイヤと呼び、ルー
 トの位置する層から順番に Layer(0)、Layer(1)、 \dots と定義する。このとき
 、受信者をリーフに割り当てられた2分木を、Layer(b) に存在するノードをル
 ートとする 2^b 個の2分木に分割し、分割された2分木に対して The Subset Dif
 ference Method を適用する。このとき、Layer(0)～Layer(b-1)に存在するノー
 ドは使用しない。

【0061】

これにより、受信者が保有しておく情報量 I_u を式（2-3）のように減らすこと

ができる。しかし、伝送情報Mの量（無効化しない受信者をカバーする部分木の数）は、無効化したい受信者数を $|\underline{R}| = r$ とすると最大で $2^b + 2r - 1$ と増加する。

【0062】

【数7】

$$1 + \sum_{k=1}^{\log_2 N - b} k = \frac{1}{2}(\log_2 N - b)^2 + \frac{1}{2}(\log_2 N - b) + 1 \quad (2-3)$$

【0063】

(1.3) 本実施形態による方法 (The Layer Division Subset Difference Method)

(1.3.1) 部分集合 $\underline{S}_1, \dots, \underline{S}_w$ の定義

最初に受信者全体の集合 \underline{N} の部分集合 $\underline{S}_1, \dots, \underline{S}_w$ を定義する。この部分集合に対して暗号（復号）鍵、又は復号鍵を導けるような情報 L_1, \dots, L_w を割り当てることになる。N枚のリーフを持つ2分木のリーフに各受信者を割り当てる（ここでNは2の冪であるとしている。）。木構造においてノードの位置する各層をレイヤと呼び、ルートの位置する層から順番に Layer(0)、Layer(1)、
 \dots と定義する。リーフの存在する層は Layer($\log_2 N$)になる。図4に示すように2分木をLayer(0)~Layer(d)、Layer(d)~Layer(2d)、 \dots といったようにd+1階層ずつのレイヤに分割する。図4ではd=2の場合を示している。分割された各層をマクロレイヤと呼ぶことにし、ルートを含むマクロレイヤから順番に MacroLayer(0)、MacroLayer(1)、 \dots 、MacroLayer($(\log_2 N)/d - 1$) と定義する。各MacroLayer(s) ($0 \leq s \leq ((\log_2 N)/d - 1)$) は、全体の2分木を分割した高さdの 2^{sd} 個の部分木 T_h から構成される。全体で上記部分木 T_h は

【数8】

$$(1 - 2^{\log_2 N}) / (1 - 2^d)$$

個存在することになる。各部分木

【数9】

$$T_h (0 \leq h \leq (2^d - 2^{\log_2 N}) / (1 - 2^d))$$

を、リーフに受信者を割り当てた2分木と考え、The Subset Difference Methodにおいて定義された差分集合を部分集合 $\underline{S}_1, \dots, \underline{S}_w$ として定義し、暗号（復号）鍵 L_1, \dots, L_w を割り当てる。（実際には、部分木 T_h のリーフは、 $s = (\log_2 N) / d - 1$ の場合（MacroLayer $((\log_2 N) / d - 1)$ 中の部分木）を除いて、全体の2分木で見た場合ただのノードであり、受信者が割り当てられているわけではない。そこで、ある任意の部分木 T_h におけるリーフには、そのリーフに対応する全体の2分木中のノード以下に存在する全てのリーフに割り当てられた受信者の集合が割り当てられていると考える。）。

【0064】

部分木 T_h 中の任意のノード v_i をルートとする部分木 $T_{h,i}$ の全てのリーフに割り当てられた受信者の集合を \underline{S}_i で表す。ノード v_i 以下のリーフに割り当てられた受信者の集合 \underline{S}_i と $T_{h,i}$ 中の（ルートを除く）ノード v_j をルートとする部分木 $T_{h,j}$ のリーフに割り当てられた受信者の集合 $\underline{S}_j \subset \underline{S}_i$ について、 \underline{S}_i の要素から \underline{S}_j の要素を引いた差分集合を $\underline{S}_{i,j}$ とする。つまり、集合 \underline{S}_i に含まれる受信者のうち、集合 \underline{S}_j に含まれていない受信者の集合を $\underline{S}_{i,j}$ とする。図5は $\underline{S}_{i,j}$ を示している。この差分集合に対して1つの暗号（復号）鍵 $L_{i,j}$ を割り当てる。

【0065】

(1.3.2) $\underline{N} \setminus \underline{R}$ の分割方法

次に受信を許可する（無効化しない）受信者の集合 $\underline{N} \setminus \underline{R}$ を、上記で定義された差分集合 $\underline{S}_{i,j}$ に分割する方法を説明する。無効化したい受信者を割り当てられているリーフ、または無効化したい受信者を1つでも含むような受信者の集合を割り当てられているリーフを含む全ての部分木 T_h について以下の処理を行う。

【0066】

無効化したい受信者を含む部分木 T_h について、部分木 T_h のルートと無効化し

たい受信者（又は無効化したい受信者を含む受信者の集合）に相当する各リーフを結ぶ最短のパス上のノードのみで構成される部分木 $ST_h(\underline{R})$ を考える（このような部分木は \underline{R} から一意に構成される）。 $ST_h(\underline{R})$ については子ノードの存在しないノードをリーフと呼ぶことにする。また、以下の(1)～(4)の処理において用いられているルートとリーフは、部分木 T_h 中のそれを表しているものとする。

【0067】

(1) 2つのリーフからルートへのパスの共通部分に存在するノードの中で、リーフとの距離が最小となるノードを2つのリーフの最小共通ノードと呼ぶことにする。 $ST_h(\underline{R})$ のリーフ v_i, v_j を、それらの最小共通ノード v 以下に他のリーフが存在しないように選ぶ。 v の2つの子ノードの中で、 v と v_i のパス上に存在する子ノードを v_k 、 v と v_j のパス上に存在する子ノードを v_l とする。

（リーフが $ST_h(\underline{R})$ 中に1つしか存在しない場合、 $v_i = v_j$ 、 $v = v_j = v_k$ として、 v を $ST_h(\underline{R})$ のルートと考えればよい。）

(2) $v_k \neq v_l$ ならば $\underline{N} \setminus \underline{R}$ を構成する差分集合に $\underline{S}_{k,i}$ を加える。 $v_l \neq v_j$ ならば $\underline{N} \setminus \underline{R}$ を構成する差分集合に $\underline{S}_{l,j}$ を加える。

【0068】

(3) v より下に位置する部分木 T_h 中のノードを全て除去する。これにより、 v がリーフになる。

【0069】

(4) $ST_h(\underline{R})$ にルート以外のノードが存在する場合、上記(1)に戻る。 $ST_h(\underline{R})$ がルートのノードのみになった場合、無効化したい受信者を含む他の部分木 T_h を選択し、上記(1)に戻って同様の処理を繰り返す。 $ST_h(\underline{R})$ がルートのノードのみなり、かつ無効化したい受信者を含む他の部分木 T_h が存在しない場合、処理を終了する。

【0070】

上記アルゴリズムにより構成された差分集合 $\underline{S}_{i,j}$ の集合が $\underline{N} \setminus \underline{R}$ を構成する差分集合の集合である。 $\underline{N} \setminus \underline{R}$ の分割数（ $\underline{N} \setminus \underline{R}$ を構成する差分集合の数）の上限は、 d の値により異なるが、例えば $d=2$ のとき（このとき、 N は4の冪である

と仮定している。) 、無効化したい受信者数 $|R| = r$ とすると式 (3-1) のようになる。

【0071】

【数10】

$$1 + \sum_{j=1}^r f_j \quad (3-1)$$

$$f_j = \begin{cases} \log_4(N) - 1 & (j = 1) \\ \log_4(N) & (j = 2) \\ \log_4(N/4^i) & (2 \cdot 4^{i-1} < j \leq 4^i) \\ \log_4(N/4^i) - 1 & (4^i < j \leq 2 \cdot 4^i \text{ かつ } j \text{ が奇数}) \\ \log_4(N/4^i) & (4^i < j \leq 2 \cdot 4^i \text{ かつ } j \text{ が偶数}) \\ -1 & (2 \cdot 4^{\log_4 N - 1} < j \leq 4^{\log_4 N} = N) \end{cases}$$

【0072】

ここで i は $0 < i < \log_4 N$ を満たす整数である。

【0073】

(1.3.3) 部分集合 S_1, \dots, S_w への鍵の割り当て方法

次に各差分集合に対する鍵の割り当て方法について説明する。各差分集合 S_i , j に対して、一様に分布しており、互いに独立な値を持つ鍵を割り当てる。各受信者には自分の属する差分集合に割り当てられた全ての鍵を配布しておく。

【0074】

(1.3.4) 受信者への秘密情報の割り当て方法

受信者 u を割り当てられたリーフと、全体の2分木のルートとのパス上に存在するノードを含む各部分木 T_h について考える。このような部分木 T_h は各マクロレイヤ中に必ず1つ存在する。パス上のノードの中で部分木 T_h に含まれる任意のノードを v_i とし、 v_i をルートとする部分木 $T_{h,i}$ のリーフに割り当てられた受信者の集合を S_i とする。部分木 $T_{h,i}$ 中のノードであり、かつパス上に存在しないノードを v_j とし、 v_j をルートとする部分木 $T_{h,j}$ のリーフに割り当てられた受信者の集合を $S_j \subset S_i$ とする。集合 S_i に含まれ、集合 S_j に含まれない受信者の集合 (差分集合) を $S_{i,j}$ で表す。このとき受信者 u は上記の全ての差分集合 $S_{i,j}$ に割り当てられた鍵を保有しておく必要がある。受信者 u の属する部分

木 T_h の数は、マクロレイヤ数に等しいから $\log_2 N/d$ 個存在する。部分木 T_h の高さは d であるから、部分木 T_h 中に存在し、かつパス上のノード v_i をルートとする部分木 $T_{h,i}$ は d 個存在する（ノード v_i が部分木 T_h のリーフに相当する場合は、受信者の集合を割り当てる必要がないため除外している。）。部分木 $T_{h,i}$ の高さを k 、($1 \leq k \leq d$) とすると、部分木 $T_{h,i}$ 中のノードで、かつパス上に存在しないノード v_j をルートとする部分木 $T_{h,j}$ は $\{(2^{k+1}-1) - (k+1)\}$ 個存在する。これより各部分木 $T_{h,i}$ について、集合 \underline{S}_j の数は $\{(2^{k+1}-1) - (k+1)\}$ 個である。よって差分集合 $\underline{S}_{i,j}$ の数は式 (3-2) のようになる。受信者 u は式 (3-2) に示すだけの個数の鍵を保有しておかなければならない。式 (3-2) において 1 が足されているのは、無効化する受信者が全く存在しない場合の鍵が必要だからである。

【0075】

【数11】

$$1 + \frac{\log_2 N}{d} \sum_{k=1}^d (2^{k+1} - k - 2) = \frac{4(2^d - 1) \log_2 N}{d} - \frac{(d+5) \log_2 N}{2} + 1 \quad (3-2)$$

【0076】

(1.3.2) 部分集合 $\underline{S}_1, \dots, \underline{S}_w$ への鍵の割り当て方法（擬似乱数生成器を用いる場合）

受信者が保有しておく鍵を減らすため、The Subset Difference Method と同様に擬似乱数生成器を用いて差分集合への鍵の割り当てを行うこともできる。つまり、各差分集合 $\underline{S}_{i,j}$ に直接鍵を割り当てるのではなく、部分木 $T_{h,i}$ のリーフに割り当てられた受信者の集合 \underline{S}_i に対して 1 つのラベルを割り当てる。このとき、差分集合 $\underline{S}_{i,j}$ ($\forall j, \underline{S}_j \subset \underline{S}_i$) に割り当てる鍵 $L_{i,j}$ が、部分集合 \underline{S}_i に割り当てられたラベルを用いて導けるようにしておく。このとき、差分集合 $\underline{S}_{i,j}$ 内に存在する受信者のみが鍵 $L_{i,j}$ を導けるようにしなければならない。以下では、擬似乱数生成器を用いて、上記方法を実現する方法を示す。

【0077】

$G: \{0, 1\}^n \rightarrow \{0, 1\}^{3n}$ を入力長の 3 倍の長さを出力する擬似

乱数生成器とする。擬似乱数生成器 G の入力を S としたとき、出力される値を 3 等分した左側部分を $G_L(S)$ で表し、右側部分を $G_R(S)$ 、中央部分を $G_M(S)$ で表す。また、 G の入力として乱数を与えたときに出力される値と、出力と同じ長さの真の乱数を多項式時間の計算能力をもつ攻撃者に与えたとき、攻撃者は、有意な確率で両者を区別できないといった特性を G は満たしていなければならない。

【0078】

ノード v_i をルートとする MacroLayer(s) 中の部分木 $T_{h,i}$ を考える。ルートノード v_i にラベル $LABEL_i$ を割り当てる（簡単のため任意の部分木のリーフに割り当てられた受信者の集合へのラベルの割り当てを、その部分木のルートノードにラベルを割り当てると表現する。つまり上記表現は次のようになる。「部分木 $T_{h,i}$ 中のリーフに割り当てられた受信者の集合 S_i にラベル $LABEL_i$ を割り当てる。」）。 $LABEL_{i,j}$ を、部分木 $T_{h,i}$ 中のノード v_j のラベルとする（割り当てられるラベルが 2 変数のパラメータを持つ場合、それは差分集合に対して割り当てられたラベルを示している。このとき、 $LABEL_{i,j}$ は v_j をルートとする部分木のリーフに割り当てられた受信者の集合 S_j に割り当てられるのではなく、 S_i に含まれ、 S_j には含まれていない受信者の集合（差分集合） $S_{i,j}$ に対して割り当てられる。）。 $LABEL_{i,j}$ が差分集合 $S_{i,j}$ に割り当てられるラベルである。 $LABEL_{i,j}$ を部分木 $T_{h,i}$ のルート v_i に割り当てられたラベル $LABEL_i$ から擬似乱数生成器 G を用いて以下の導出規則により導く。

【0079】

ラベルを擬似乱数生成器の入力としたとき、その出力を次のように定義する。 G_L —左側の子ノードのラベル、 G_R —右側の子ノードのラベル、 G_M —入力ラベルの割り当てられたノードに割り当てる暗号（復号）鍵。この導出規則に拠れば、部分木 $T_{h,i}$ 中のある親ノードにラベル S が割り当てられたとき、その 2 つの子ノードのラベルは、 $G_L(S)$ 、 $G_R(S)$ が割り当てられる。これより、 v_i から v_j に至るパス上のノードに割り当てるラベルを G を用いて順次求めることで、 v_i に割り当てられたラベル $LABEL_i$ から、部分木 $T_{h,i}$ 中のノード v_j のラベル $LABEL_{i,j}$ を求めることができる。最後に $LABEL_{i,j}$ を G の入力としたときの出力

の中央部分 $G_M(\text{LABEL}_{i,j})$ を、差分集合 $S_{i,j}$ に割り当てる暗号（復号）鍵 $L_{i,j}$ として用いる。図6に差分集合 $S_{i,j}$ に割り当てる鍵 $L_{i,j}$ の割り当て例を示す。

【0080】

このような方法を用いれば、部分木中のあるノードのラベルが与えられたとき、部分木内でのその子孫ノード全てのラベルと暗号（復号）鍵を計算することができる。逆に、あるノード v_j の先祖ノードのラベルを v_j から求めることはできない。さらに、ノード v_j の全ての子孫ノードのラベル（ただし、 v_j 自身のラベルは含まない）から暗号（復号）鍵 $L_{i,j}$ を求めることはできない。部分木 $T_{h,i}$ のルートのラベル LABEL_i が与えられたとき、差分集合 $S_{i,j}$ に割り当てられる暗号（復号）鍵 $L_{i,j}$ を計算するのに擬似乱数生成器 G を最大で $d+1$ 回用いる。

【0081】

(1.3.6) 受信者への秘密情報の割り当て方法（擬似乱数生成器を用いる場合）

各受信者 u が保有する秘密情報 I_u の割り当て方法について説明する。各マクロレイヤ中に1つずつ存在する u の属する部分木 T_h について考える。部分木 T_h のルートと u の割り当てられたリーフを結ぶパス上の d 個（リーフ部分のノードは数えていない。）のノードを v_i とし、 v_i をルートとする高さ k 、($1 \leq k \leq d$) の部分木 $T_{h,i}$ のノードの中で、パスに直接ぶら下がるノードを v_{i1} 、 v_{i2} 、 \dots 、 v_{ik} で表す（図7）。つまり、それらは部分木 $T_{h,i}$ 中のノードの中で、パスに隣接し、かつ u の先祖ノードでないノードである。部分木 $T_{h,i}$ 中のノードで、 u の先祖でない任意のノード v_j は、これらのノード v_{i1} 、 v_{i2} 、 \dots 、 v_{ik} のいずれかの子孫ノードである。ゆえに、受信者 u が I_u として、 v_{i1} 、 v_{i2} 、 \dots 、 v_{ik} に割り当てられたラベルを保有しておけば、最大 $d+1$ 回擬似乱数生成器 G を用いて、部分木 $T_{h,i}$ 中でパス上に存在しない任意ノード v_j に割り当てられた復号鍵 $L_{i,j}$ を計算することができる。

【0082】

受信者 u を含む部分木 T_h の数は、マクロレイヤ数に等しいから $\log_2 N/d$ であり、部分木 T_h 中にパス上のノードをルートとする部分木 $T_{h,i}$ は d 個存在する。高さ k の部分木 $T_{h,i}$ 中に受信者 u が保有しなければならないラベルは k 個ある

から、これを u を含む各部分木 $T_{h,i}$ について考えると、受信者 u が保有しておかなければならない復号鍵（ラベル）の数は式（3-3）のようになる。

【0083】

【数12】

$$1 + \frac{\log_2 N}{d} \sum_{k=1}^d k = \frac{(d+1) \log_2 N}{2} + 1 \quad (3-3)$$

【0084】

式（3-3）において1が足されているのは、式（3-2）と同様に無効化する受信者が全く存在しない場合の復号鍵が必要だからである。擬似乱数生成器を用いて差分集合への鍵の割り当てを行った場合、受信者の保有する秘密情報は復号鍵ではなく各部分木 $T_{h,i}$ に割り当てられたラベルであるが、受信者を全く無効化しない場合に用いる復号鍵については鍵そのものを保有することになる。

【0085】

（1.3.7）複数の2分木を用いる方法

さらに受信者 u が保有する秘密情報 I_u を減らす場合は、伝送情報 M の量とのトレードオフとなる。一つの方法として、2分木を高さの低い木に限定して複数用いる方法がある。受信者をリーフに割り当てられた2分木を、Layer(b)に存在するノードをルートとする 2^b 個の2分木に分割し、分割された2分木に対して本方式を適用する。このとき、Layer(0) ~ Layer(b-1)に存在するノードは使用しない。これにより、受信者が保有しておく情報量 I_u を式（3-4）、式（3-5）のように減らすことができる。擬似乱数生成器を用いない場合の復号鍵（ラベル）保有数が、式（3-4）であり、擬似乱数生成器を用いる場合のそれが式（3-5）である。式（3-4）、式（3-5）において共に1が足されているのは、自身の割り当てられているリーフの属する2分木中に、無効化する受信者が全く存在しない場合の鍵が必要だからである。

【0086】

【数 13】

$$1 + \frac{\log_2 N - b}{d} \sum_{k=1}^d (2^{k+1} - k - 2) = \frac{4(2^d - 1)(\log_2 N - b)}{d} - \frac{(d+5)(\log_2 N - b)}{2} + 1 \quad (3-4)$$

$$1 + \frac{\log_2 N - b}{d} \sum_{k=1}^d k = \frac{(d+1)(\log_2 N - b)}{2} + 1 \quad (3-5)$$

【0087】

伝送情報Mの量（無効化しない受信者をカバーする部分木の数）の上限は、例としてd=2のときを考えると、無効化したい受信者数が $|\underline{R}| = r$ のとき式（3-6）のようになる。

【0088】

【数 14】

$$4^h + \sum_{j=1}^r f_j \quad (3-6)$$

$$f_j = \begin{cases} \log_4(N/4^h) - 1 & (0 < j \leq 2 \cdot 4^h \text{ かつ } j \text{ が奇数}) \\ \log_4(N/4^h) & (0 < j \leq 2 \cdot 4^h \text{ かつ } j \text{ が偶数}) \\ \log_4(N/4^{h+i}) & (2 \cdot 4^{h+i-1} < j \leq 4^{h+i}) \\ \log_4(N/4^{h+i}) - 1 & (4^{h+i} < j \leq 2 \cdot 4^{h+i} \text{ かつ } j \text{ が奇数}) \\ \log_4(N/4^{h+i}) & (4^{h+i} < j \leq 2 \cdot 4^{h+i} \text{ かつ } j \text{ が偶数}) \\ -1 & (2 \cdot 4^{\log_4 N - 1} < j \leq 4^{\log_4 N} = N) \end{cases}$$

【0089】

ここで i は $0 < i < \log_4(N/4^h)$ を満たす整数である。

【0090】

(1.4) 各方式の性能比較

図8に受信者総数 $|\underline{N}|$ 、無効化したい受信者数 $|\underline{R}| = r$ を一定にしたとき、各方式において受信者が保有しておく秘密情報と伝送するヘッダー量の関係を示す。図8に示すように、 $\underline{N} = 2^{30} = 1,073,741,824 \div 10$ 億、 $r = 2^{14} = 16,384$ とし、各方式で用いる暗号化アルゴリズムの鍵長は全て128bitとした。

【0091】

横軸が受信者の保有しておく秘密情報量、縦軸が伝送するヘッダー量の上限を表しており、グラフの左下にある方式ほど、伝送又は蓄える情報量が少ないため、この2点に関しては優れた方式といえる。

【0092】

実際のシステムの運用においては、受信者 u は自身が保有する秘密情報 I_u から、どの復号鍵 (The Subset Difference Method、The Layer Division Subset Difference Methodで擬似乱数生成器を使用する場合はラベル情報) を用いて、伝送されたヘッダー情報を復号するのかを決定する必要がある。その方法としては、例えば、全ての復号鍵で全てのヘッダー情報を復号する方法や、復号に使用すべき復号鍵の情報 (ヘッダーの暗号化に使用した暗号鍵のインデックス情報) を付与する方法などが考えられる。この場合伝送される情報はさらにインデックス情報分増加することになるが、図8では考慮していない。

【0093】

The Subset Difference Methodは全部で19点 (丸で示す) プロットされているが、これは、変数 b をパラメータとしているためである。左の点から $h=18, 17, \dots, 1, 0$ となっており、一番右端の点が2分木を1つのみ用いた方式に相当する。また、差分集合へのラベルの割り当ては、擬似乱数生成器を用いた方式のみを表示している。

【0094】

New Method と書かれた方式が本発明の実施形態による方法 (The Layer Division Subset Difference Method) であり、これは、差分集合へのラベルの割り当てに擬似乱数生成器を用いていない。本発明の実施形態による方法で擬似乱数生成器を用いた方式は、New Method using PRNG と書かれた方式である。

【0095】

それぞれ複数の点がプロットされているのは、変数 d をパラメータとしているためで、左から $d=1, 2, \dots$ のときを表している。 $d=1$ のときは擬似乱数生成器を用いたラベルの割り当てを行っても (受信者が保有する秘密情報量削減という意味での) 性能は向上しないことがわかる。また、The Subset Difference

Method と同様に b を変数とすることもできるが、ここでは各 d について、伝送するヘッダー量が最小となるパラメータの中で、受信者の保有する秘密情報量が最も少なくなるような b のみを選択して、その場合のみを表示している。図8には表示していないが、 $d=1$ 、 $b=0$ の場合、アルゴリズムが The Complete Subtree Method と完全に等価になる。 $d=16$ 、 $b=14$ の場合は、The Subset Difference Method の $h=14$ とした場合と等価になる（図8で2つの方式の結果が重なっている点）。The Tree Pattern Division Method については、アルゴリズムに使用する木を2分木のみでなく任意の n 分木を用いる。そのため、図8には、左から使用する木を2分木、3分木、4分木、5分木とした場合の結果を表示している。 n 分木のリーフに受信者を割り当てるため、2分木、4分木を用いる場合を除いて、受信者総数は $2^{30} = 4^{15} = 1,073,741,824$ にならない。よって、3分木、5分木については以下の値を用いた。

【0096】

- ・ 3分木： $N = 3^{19} = 1,162,261,467 \approx 10$ 億
- ・ 5分木： $N = 5^{13} = 1,220,703,125 \approx 10$ 億

また、2分木のとき The Complete Subtree Method とアルゴリズムが完全に等価である。

【0097】

(1.5) 実施形態のコンテンツ配信システム

本発明の実施形態によるコンテンツ配信システムの概略構成を図1(b)に示す。このシステムは、情報提供者7が各種の記憶媒体9をユーザに提供する。本実施形態では、記憶媒体9は、例えばDVD-ROMなどの光ディスクを含む各種の記録媒体とすることが可能である。ユーザは再生装置8を所持し、当該再生装置8により記録媒体9から情報を再生する。再生装置8は内部に復号鍵4aを有している。

【0098】

ここで、情報提供者7は上記の鍵管理方式の3要素における情報送信者に対応し、再生装置8は情報受信者に対応する。即ち、情報提供者7は、映像／音声などのコンテンツ情報を暗号化用鍵情報5を使用して暗号化し、伝送情報6として

記録媒体 9 に記録する。また、情報提供者 7 は、無効化の対象となる再生装置 8 によっては復号できないが、無効化の対象とならない再生装置 8 によれば復号可能な鍵情報 4 b を記録媒体 9 に記録する。そして、情報提供者 7 は記録媒体 9 を各再生装置 8 のユーザに提供する。

【 0 0 9 9 】

無効化の対象とならない再生装置 8 は、自己の有する復号用鍵 4 a で鍵情報 4 b を復号して伝送情報 6 の復号鍵を取得し、これで伝送情報 6 を復号して映像／音声などの情報を再生することができる。一方、無効化の対象となる再生装置 8 は、自己の復号用鍵 4 a により記録媒体 9 内の鍵情報 4 b を復号することができないので、伝送情報 6 を復号する鍵を得ることができず、伝送情報 6 を再生することができない。こうして、本システムでは、記録媒体 9 上に記録された伝送情報 6 を特定の再生装置 8 のみにより再生可能とする。

【 0 1 0 0 】

本発明では、上述の階層分割を伴う鍵管理方式 (The Layer Division Subset Difference Method) に従って、再生装置 8 側の復号用鍵 4 a 及び記録媒体 9 に記録される鍵情報 4 b を生成する。具体的には、ある再生装置 8 に対して、その再生装置を含むような全ての差分集合に割り当てられている復号鍵 (または復号鍵を導けるようなラベル) と、当該再生装置が割り当てられたリーフの属する 2 分木のルートに割り当てられた復号鍵 1 つを当該再生装置に復号用鍵 4 a として配布すればよい。こうして、記録媒体中 9 の鍵情報 4 b の情報量の増加を押さえつつ、再生装置 8 に保持しておく復号用鍵 4 a の情報量を大幅に減少させることができる。

【 0 1 0 1 】

【実施例】

次に、本発明の実施例に係るコンテンツ配信システムについて説明する。なお、このコンテンツ配信システムは、DVD などの光ディスクを記録媒体として使用するものであり、ここでは特に DVD-ROM を例にとって説明する。このコンテンツ配信システムでは、情報送信者はコンテンツの著作権者、光ディスク製造工場などに相当する。一方、情報受信者はコンテンツの再生機能を有する装置

(再生装置)であり、ハードウェア又はソフトウェアにより構成されている。

【0102】

なお、以下の実施例の説明において、Encryption () は暗号化アルゴリズム、Decryption () は復号化アルゴリズムを表すものとする。また、Encryption (引数1、引数2) は引数2を暗号鍵として引数1を暗号化した暗号文を表し、Decryption (引数1、引数2) は引数2を復号鍵として引数1を復号したデータを表す。また、記号“|”は2つのデータの結合を表し、(データA) | (データB) のように用いる。

【0103】

(2.1) コンテンツ記録装置

まず、コンテンツ記録装置について説明する。図9はコンテンツをディスクに記録するコンテンツ記録装置50の構成を示すブロック図であり、情報送信者としての前述のディスク製造工場などに設けられるものである。また、コンテンツ記録装置50の各部の信号S1～S7の内容を図10及び図11に示している。なお、ここでのコンテンツは、情報送信者から情報受信者へ送信される前述の伝送情報に対応するものである。

【0104】

図9において、コンテンツ入力装置51はコンテンツを入力する装置であり、図10(a)に示すように、コンテンツに対応する信号S1を出力する。コンテンツとしては、通常、音楽、映像などのマルチメディアデータが代表的であるが、ここでのコンテンツはそれらに限定されるものではなく、文書などのデータも含まれる。また、コンテンツ入力装置51としては、コンテンツのマスターデータが記録された磁気テープや、DVD-R、DVD-RW、DVD-ROM、DVD-RAMなどの記録媒体を読み込んで信号S1を出力する回路や、LAN、インターネットなどの通信回線を経由してアクセスし、そのデータをダウンロードして信号S1を出力する回路などが挙げられる。

【0105】

復号鍵入力装置52はコンテンツ復号用の鍵Aを入力する装置であり、図10(b)に示すように、コンテンツ復号鍵Aである信号S2を出力する。コンテン

ツ復号鍵Aは、情報送信者である著作権者、ディスク製造工場又は鍵管理機関により決定される。

【0106】

暗号鍵入力装置53は、コンテンツ暗号鍵Aを入力する装置であり、図10(c)に示すように、コンテンツ暗号鍵Aである信号S3を出力する。コンテンツ暗号鍵Aとコンテンツ復号鍵Aには、次の関係が成立することが要求される。

【0107】

$P = \text{Decryption}(\text{Encryption}(\text{任意のデータ } P, \text{ コンテンツ暗号鍵 } A), \text{ コンテンツ復号鍵 } A)$

コンテンツ暗号化装置54は、コンテンツ暗号鍵A(信号S3)を用いてコンテンツ(信号S1)を暗号化し、暗号化コンテンツである信号S4を出力する。図10(d)に示すように、 $\text{信号 } S4 = \text{Encryption}(\text{コンテンツ}, \text{ コンテンツ暗号鍵 } A)$ である。

【0108】

なお、この例ではコンテンツ暗号鍵Aを用いてコンテンツを直接暗号化しているが、コンテンツ自体を暗号化する必要は必ずしもない。例えば、コンテンツ自体は他の暗号鍵Cで暗号化し、暗号鍵Cに対応する復号鍵Cを上記のコンテンツ暗号鍵Aで暗号化して信号S4として出力してもよい。つまり、ここでいう「コンテンツ暗号鍵を用いてコンテンツを暗号化する」とは、コンテンツの復号化に少なくともコンテンツ復号鍵Aを必要とするような方法でコンテンツを変換することを意味する。

【0109】

暗号鍵入力装置55は、コンテンツ復号鍵Aを暗号化するための複数の暗号鍵 B_i を入力する装置であり、N個の暗号鍵 $B_1, B_2, \dots, B_{N-1}, B_N$ を、前述の階層分割を伴う鍵管理方式のアルゴリズムに従って選択し、信号S5を出力する。図10(e)に示すように、 $\text{信号 } S5 = \text{暗号鍵 } B_1 | \text{暗号鍵 } B_2 | \dots | \text{暗号鍵 } B_i | \dots | \text{暗号鍵 } B_{N-1} | \text{暗号鍵 } B_N$ で表される。これら複数の暗号鍵 B_i の組み合わせにより、コンテンツを再生することができる再生装置(上述した「無効化の対象とならない受信者」)が一意に決まる。よって、暗号鍵 B_i は再生

を許可する権限を持つ機関（鍵管理機関又は情報送信者）が暗号鍵 B_i を決定する。

【 0 1 1 0 】

鍵暗号化装置 5 6 は、信号 S_5 として得られる暗号鍵 B_i を用いて、信号 S_2 として得られるコンテンツ復号鍵 A を暗号化し、それにヘッダー情報 Header （暗号鍵 B_i ）を付加して信号 S_6 として出力する。図 1 1（a）に示すように、

信号 $S_6 =$

$$\begin{aligned} & \text{Header (暗号鍵 } B_1) \mid \text{Encryption (コンテンツ復号鍵 } A, \text{ 暗号鍵 } B_1)) \\ & \mid \text{Header (暗号鍵 } B_2) \mid \text{Encryption (コンテンツ復号鍵 } A, \text{ 暗号鍵 } B_2)) \\ & \mid \dots \\ & \mid \text{Header (暗号鍵 } B_i) \mid \text{Encryption (コンテンツ復号鍵 } A, \text{ 暗号鍵 } B_i) \\ & \mid \dots \\ & \mid \text{Header (暗号鍵 } B_{N-1}) \mid \text{Encryption (コンテンツ復号鍵 } A, \text{ 暗号鍵 } B_{N-1}) \\ & \mid \text{Header (暗号鍵 } B_N) \mid \text{Encryption (コンテンツ復号鍵 } A, \text{ 暗号鍵 } B_N) \end{aligned}$$

で表される。なお、以下の説明では簡単のため、

信号 $S_6 = \text{Header (暗号鍵 } B) \mid \text{Encryption (コンテンツ復号鍵 } A, \text{ 暗号鍵 } B)$ と表す。

【 0 1 1 1 】

記録信号生成装置 5 7 は、暗号化されたコンテンツと、複数の暗号鍵 B_i で暗号化されたコンテンツ復号鍵 A の組み合わせとを合成して記録信号を生成する。より具体的には、記録信号生成装置 5 7 は、信号 $S_4 = \text{Encryption (コンテンツ, コンテンツ暗号鍵 } A)$ と、信号 $S_6 = \text{Header (暗号鍵 } B) \mid \text{Encryption (コンテンツ復号鍵 } A, \text{ 暗号鍵 } B)$ を結合し、それにエラー訂正符号を付加したものを信号 S_7 として出力する。よって、図 1 1（b）に示すように、信号 S_7 は、コンテンツ暗号鍵 A で暗号化したコンテンツ、 N 個の暗号鍵 B_i で暗号化されたコンテンツ復号鍵 A 及びヘッダーにエラー訂正符号を追加した信号であり、

$$\begin{aligned} S_7 = & \text{Header (暗号鍵 } B) \mid \text{Encryption (コンテンツ復号鍵 } A, \text{ 暗号鍵 } B) \\ & \mid \text{Encryption (コンテンツ, コンテンツ暗号鍵 } A) \mid \text{ECC} \end{aligned}$$

で示される。なお、 ECC はエラー訂正符号である。

【0112】

記録装置58は、生成された記録信号S7を光ディスクDに記録し、又は、光ディスクを製造するためのマスターディスクなどに記録信号S7をカッティングする）に記録する装置であり、通常レーザ光源やレーザ発信器などを備える。

【0113】

(2.2) コンテンツ再生装置

次に、上述のようにしてコンテンツが記録された光ディスクDからコンテンツを再生するためのコンテンツ再生装置60について説明する。図12はコンテンツ再生装置60の構成を示すブロック図である。また、コンテンツ再生装置60の各部の信号の内容を図13及び図14に示している。

【0114】

図12において、情報読取装置61は光ピックアップなどの装置であり、光ディスクDに記録されている情報を読み取って信号S11を出力する。信号S11は、図13(a)に示すように、

$S11 = \text{Header (暗号鍵} B) \mid \text{Encryption (コンテンツ復号鍵} A, \text{暗号鍵} B) \mid \text{Encryption (コンテンツ, コンテンツ暗号鍵} A) \mid \text{ECC}$
で表される。

【0115】

エラー訂正装置62は、入力された信号S11のエラー訂正を行う装置であり、信号S11中のECCに基づいてエラー訂正処理を実行する。そして、エラー訂正後の信号を信号S12と信号S13に分けてそれぞれ鍵復号装置64及びコンテンツ復号装置65へ供給する。信号S12は暗号鍵 B_j で暗号化されたコンテンツ復号鍵Aのデータであり、 $S12 = \text{Header (暗号鍵} B) \mid \text{Encryption (コンテンツ復号鍵} A, \text{暗号鍵} B)$ で示される。一方、信号S13はコンテンツ暗号鍵Aで暗号化されたコンテンツのデータであり、 $S13 = \text{Encryption (コンテンツ, コンテンツ暗号鍵} A)$ で示される。

【0116】

記憶装置63は、再生装置が保有する複数の復号鍵 $B_1, B_2, \dots, B_j, B_{M-1}, B_M$ とそのヘッダHeader(B_1)、Header(B_2)、 \dots 、Header(B_j)

）、・・・、Header (B_{M-1})、Header (B_M) を保存しておく装置である。なお、ここでは記憶装置 6 3 は M 個の復号鍵を保有していると仮定する。また、鍵管理機関は、コンテンツ復号鍵 A の暗号化用の暗号鍵 B_i と再生を許可されている再生装置の保有する復号鍵 B_j のうちの少なくとも 1 つは次の関係が整理するように、予め再生装置に復号鍵 B_j を配布している：

$$P = \text{Decryption} (\text{Encryption} (\text{任意のデータ } P, \text{暗号鍵 } B_i), \text{復号鍵 } B_j)$$

さらに、ヘッダーについては、上記の関係の暗号鍵 B_i と復号鍵 B_j に付加されたヘッダーについて次の関係が成立するようにヘッダーの値が決定されている：

$$\text{Header} (\text{暗号鍵 } B_i) = \text{Header} (\text{暗号鍵 } B_j)$$

上記の関係が成立するように復号鍵 B_j とそのヘッダーを各再生装置に（再生装置製造時に）配布するのは、上述の鍵管理機関であり、その際にどの再生装置にどの復号鍵 B_j を配布するかは決定は、上述の階層分割を伴う鍵管理方式のアルゴリズムに従って行われる。なお、上述のアルゴリズム中の差分集合への鍵の割り当てにおいて、疑似乱数生成器が用いられる場合は、コンテンツ再生装置 6 0 の記憶装置 6 3 に保有されるのは復号鍵 B_j そのものではなく、復号鍵を計算するのに必要なラベル情報である。

【 0 1 1 7 】

記憶装置 6 3 は、図 1 4 (b) に示すように、復号鍵 B_1 | 復号鍵 B_2 | ... | 復号鍵 B_{M-1} | 復号鍵 B_M と、そのヘッダー Header (復号鍵 B_1) | Header (復号鍵 B_2) | ... | Header (復号鍵 B_{M-1}) | Header (復号鍵 B_M) を出力する。

【 0 1 1 8 】

鍵復号装置 6 4 は、信号 $S 1 2 = \text{Header} (\text{復号鍵 } B | \text{Encryption} (\text{コンテンツ復号鍵 } A, \text{暗号鍵 } B))$ と、信号 $S 1 4 = (\text{復号鍵 } B_1 | \text{復号鍵 } B_2 | \dots | \text{復号鍵 } B_{M-1} | \text{復号鍵 } B_M)$ とそのヘッダー Header (復号鍵 B_1) | Header (復号鍵 B_2) | ... | Header (復号鍵 B_j) | ... | Header (復号鍵 B_{M-1}) | Header (復号鍵 B_M) を入力とし、光ディスク D から読み取った Header (暗号鍵 B_i) と再生装置が保有する Header (復号鍵 B_j) が一致するかを調べ、一致する時には復

号鍵 B_j を用いてEncryption (コンテンツ復号鍵A, 暗号鍵 B_i) を復号する。つまり、コンテンツ復号鍵A=Decryption (Encryption (コンテンツ復号鍵A, 暗号鍵 B_i), 復号鍵 B_j) となる。この処理を一致するヘッダーの組み合わせが見つかるように i 及び j の組み合わせを変えて実行し、図14(c)に示すように信号S15=コンテンツ復号鍵Aを出力する。一方、一致するヘッダーの組み合わせがない場合は、再生不可能として全ての処理を終了する。

【0119】

なお、前述のように記憶装置63に復号鍵 B_j そのものではなく、復号鍵を計算するのに必要なラベル情報が保存されている場合は、鍵復号装置64がラベル情報から復号鍵を計算した上で同様の処理を行えばよい。こうして、復号されたコンテンツ復号鍵Aが信号S15としてコンテンツ復号装置65へ供給される。

【0120】

コンテンツ復号装置65は、図14(a)に示す信号S13=Encryption (コンテンツ, コンテンツ暗号鍵A) と、図14(c)に示す信号S15=Decryption (Encryption (コンテンツ復号鍵A, 暗号鍵 B_i), 復号鍵 B_j) =コンテンツ復号鍵Aを入力とし、信号S15を用いて信号S13を復号し、その結果、Decryption (Encryption (コンテンツ, コンテンツ暗号鍵A), コンテンツ復号鍵A) =コンテンツを信号S16として出力する。再生装置66はコンテンツ復号装置65により復号されたコンテンツを再生する。こうして、再生を許可された再生装置のみによりコンテンツの再生が行われる。

【0121】

(2.3) コンテンツ記録処理

次に、光ディスクDへのコンテンツ記録処理について図15を参照して説明する。図15はコンテンツ記録処理のフローチャートである。まず、複数存在する再生装置の中で、対象となる光ディスクDの再生を許可する1つ以上の再生装置を選択する(ステップS1)。この処理は、通常は鍵管理機関により行われるが、著作権者、ディスク製造工場などの情報送信者が行う場合もある。

【0122】

次に、ステップS1で選ばれた、再生を許可する再生装置全てについて、少な

くとも1つは復号鍵が存在し、かつ、再生を許可されていない装置については1つも復号鍵が存在しないような復号鍵の集合のうち最小となる集合を選択する（ステップS2）。

【0123】

次に、コンテンツ復号鍵Aを決定し、ステップS2で選択された復号鍵の集合に属する全ての復号鍵 B_j を、 $P = \text{Decryption}(\text{Encryption}(\text{任意のデータ } P, \text{暗号鍵 } B_j))$ 、復号鍵 B_j を満たす暗号鍵 B_i を用いて暗号化し、 $\text{Encryption}(\text{コンテンツ復号鍵 } A, \text{暗号鍵 } B_i)$ を求める（ステップS3）。通常、この処理も鍵管理機関で行われるが、情報送信者が行う場合もある。

【0124】

次に、ステップS3で選択されたコンテンツ暗号鍵Aを用いてコンテンツを暗号化し、 $\text{Encryption}(\text{コンテンツ}, \text{コンテンツ暗号鍵 } A)$ を求める（ステップS4）。この処理は、通常、情報送信者が行う。

【0125】

次に、ステップS3及びS4で求められた $\text{Encryption}(\text{コンテンツ復号鍵 } A, \text{暗号鍵 } B_i)$ 及び $\text{Encryption}(\text{コンテンツ}, \text{コンテンツ暗号鍵 } A)$ に対してエラー訂正符号を付加する（ステップS5）。この処理は、情報送信者である著作権者、ディスク製造工場などで行われる。

【0126】

そして、ステップS3、S4及びS5で計算された $\text{Encryption}(\text{コンテンツ復号鍵 } A, \text{暗号鍵 } B_i)$ 及び $\text{Encryption}(\text{コンテンツ}, \text{コンテンツ暗号鍵 } A)$ 並びにエラー訂正符号を光ディスクDに記録する（ステップS6）。この処理はディスク製造工場など、情報送信者により行われる。こうして、暗号化されたコンテンツ及びその復号鍵の情報が光ディスクDに記録される。

【0127】

次に、上記ステップS2における復号鍵の集合の選択処理について図16を参照して説明する。図16は、図15におけるステップS2の処理、即ち、再生を許可しない再生装置が与えられたとき、対象ディスクの再生を許可された再生装置の全てについて1つの復号（暗号）鍵が存在し、かつ、再生を許可されてい

い装置については1つも復号（暗号）鍵が存在しないような復号（暗号）鍵の集合のうち、最小となる集合を選択する処理を詳細に示すフローチャートである。

【0128】

まず、複数の再生装置をそれぞれリーフに割り当てた 2^b 個の2分木から、無効化したい（再生を許可しない）再生装置の存在しない2分木について、そのルートに割り当てられた暗号鍵を暗号鍵 B_i として選択する（ステップS21）。このとき、無効化したい再生装置の存在しない2分木は除去し、その後の処理の対象から除外する。

【0129】

次に、2分木が存在するか否かを判定する（ステップS22）。存在する場合、無効化したい再生装置又は無効化したい再生装置を含む再生装置の集合の割り当てられているリーフ（この2種類のリーフをまとめて「無効化リーフ」と呼ぶ。）を含む任意の部分木 T_h を1つ選び、 $ST_h(\underline{R})$ を構成する（ステップS23）。ここで、 $ST_h(\underline{R})$ とは、部分木 T_h のルートと無効化リーフを結ぶ最短パス上のノードのみで構成される部分木のことである。また、ここで選択される部分木 T_h はどの2分木中に含まれていても構わない。つまり、ステップS21で除去されなかった全ての2分木が対象となっている。

【0130】

次に、 $ST_h(\underline{R})$ 中の1つの無効化リーフ v_i 、 v_j を、それらの共通ノード v 以下に他の無効化リーフが存在しないように選択する（ステップS24）。ここで共通ノードとは、2つの無効化リーフからルートへのパスの共通部分に存在するノードの中で無効化リーフとの距離が最小となるノードのことである。 v の2つの子ノードの中で、 v と v_i のパス上に存在する子ノードを v_k 、 v と v_j のパス上に存在する子ノードを v_l とする。（無効化リーフが $ST_h(\underline{R})$ 中に1つしか存在しない場合、 $v_i = v_j$ 、 $v = v_l = v_k$ とし、 v は $ST_h(\underline{R})$ のルートとなっている。

【0131】

次に、 $v_i \neq v_k$ ならば、差分集合 $S_{k,i}$ に割り当てられた暗号鍵を B_i の1つとして選択する（ステップS25）。同様に、 $v_l \neq v_j$ の場合も差分集合 $S_{l,j}$ に

割り当てられた暗号鍵を B_i の 1 つとして選択する。差分集合への鍵の割り当てに疑似乱数生成器を用いている場合は、集合 S_k 、 S_l に割り当てられたラベルから、前述の方法により差分集合 $S_{k,i}$ 、 $S_{l,j}$ に割り当てられている暗号鍵を計算し、暗号鍵を B_i の 1 つとして選択する。

【0132】

次に、ノード v より下に位置する部分木 T_h 中のノードを全て除去し、 v を無効化リーフとする（ステップ S 2 6）。次に、 $ST_h(R)$ 内のルートノードが無効化リーフであるか否かを判定し（ステップ S 2 7）。ルートノードが無効化リーフである場合は、ルートノード以外に無効化リーフを含む他の部分木 T_h が全ての 2 分木中に存在するか否かを判定する（ステップ S 2 8）。存在する場合、処理はステップ S 2 3 に戻り、ルートノード以外に無効化リーフを含む他の部分木 T_h を選択し、同様の処理を繰り返す。

【0133】

一方、ステップ S 2 7 で $ST_h(R)$ 内のルートノードが無効化リーフでないと判定された場合、処理はステップ S 2 4 へ戻り他の無効化リーフを選択して同様の処理を行う。

【0134】

こうして、ルートノード以外に無効化リーフを含む他の部分木 T_h が全ての 2 分木中に存在しなくなったとき（ステップ S 2 8 ; No）、処理は終了する。コンテンツ復号鍵 A の暗号化に用いられる暗号鍵 B_i の集合は、ステップ S 2 1 及びステップ S 2 5 で選択され（又はラベルから計算）された暗号鍵となる。

【0135】

(2.4) コンテンツ再生処理

次に、光ディスク D からのコンテンツ再生処理について説明する。図 1 7 はコンテンツ再生処理のフローチャートである。まず、光ディスク D から光ピックアップなどの読取装置 6 1 により記録情報が読み取られる（ステップ S 3 1）。次に、ステップ S 3 1 で得られた信号に対してエラー訂正装置 6 2 によりエラー訂正を行う（ステップ S 3 2）。

【0136】

次に、光ディスクD中に記録されているN個のヘッダーHeader (暗号鍵 B_i) の中に、再生装置が保有するM個の復号鍵 B_j のヘッダーHeader (復号鍵 B_j) の少なくとも1つは一致するものが存在するか否かを調べる (ステップS33) 。存在する場合、その再生装置は再生を許可されたものであることになり、一致した光ディスクD側のヘッダーHeader (暗号鍵 B_i) に対応するEncryption (コンテンツ復号鍵A, 暗号鍵 B_i) を、再生装置側のヘッダーHeader (復号鍵 B_j) に対応する復号鍵 B_j で復号する (ステップS34) 。つまり、コンテンツ復号鍵A=Decryption (Encryption (コンテンツ復号鍵A, 暗号鍵 B_i) , 復号鍵 B_j) という処理を行い、コンテンツ復号鍵Aを得る。

【0137】

次に、ステップS34で復号されたコンテンツ復号鍵Aを用いて、光ディスクD上の暗号化コンテンツであるEncryption (コンテンツ, コンテンツ暗号鍵A) を復号する (ステップS35) 。つまり、コンテンツ=Decryption (Encryption (コンテンツ, コンテンツ暗号鍵A) , コンテンツ復号鍵A) という処理を行い、コンテンツの復号を行う。そして、復号されたコンテンツを再生する (ステップS36) 。

【0138】

なお、ステップS33で一致するヘッダーが見つからない場合は (ステップS33; No) 、その再生装置による再生が許可されていないことになり、コンテンツの再生は行われず、処理は終了する。

【0139】

(2.5) 差分集合への暗号鍵の割り当てに疑似乱数生成器を使用する場合

次に、本発明による階層分割を伴う鍵管理方式において差分集合へ暗号 (復号) 鍵を割り当てる際に疑似乱数生成器を用いる場合の処理を図18のフローチャートを参照して説明する。

【0140】

まず、 2^b 個の各2分木のルートに独立な値をもつ暗号 (復号) 鍵を割り当てる (ステップS41) 。次に、 2^b 個の2分木中に含まれる全てのノードに独立な値を持つラベルを割り当てる (ステップS42) 。但し、1台の再生装置のみ

が割り当てられているノード（リーフ）は除外される。そして、任意の部分木 T_h を選択し（ステップS43）、選択された部分木 T_h 中の任意のノード v_i をルートとする部分木 $T_{h,i}$ を選択する（ステップS44）。

【0141】

次に、ステップS44で選択された部分木 $T_{h,i}$ のルートノードに割り当てられたラベル $LABEL_i$ （ステップS42で割り当てられている）を用いて、差分集合 $S_{i,*}$ に暗号（復号）鍵 $L_{i,*}$ を割り当てる（ステップS45）。ここで、 $*$ は部分木 $T_{h,i}$ 中の任意のノード v_* を表す。（但し、 $T_{h,i}$ のルートノード v_i は除く）。各差分集合への暗号（復号）鍵の割り当ては以下のように行う。

【0142】

始めに疑似乱数生成器 G の入力をラベル $LABEL_{i,*}$ としたとき、その出力を3等分した左側部分を $G_L(LABEL_{i,*})$ 、中央部分を $G_M(LABEL_{i,*})$ 、右側部分を $G_R(LABEL_{i,*})$ で表す。このとき各出力を以下のように定義する。

【0143】

$G_L(LABEL_{i,*})$ 入力ラベル $LABEL_{i,*}$ の割り当てられたノードの左側の子ノードに割り当てるラベル

$G_M(LABEL_{i,*})$ 入力ラベル $LABEL_{i,*}$ の割り当てられたノードに割り当てる暗号鍵 $L_{i,*}$ （これが差分集合 $S_{i,*}$ に割り当てられる暗号（復号）鍵になる）

$G_R(LABEL_{i,*})$ 入力ラベル $LABEL_{i,*}$ の割り当てられたノードの右側の子ノードに割り当てるラベル

部分木 $T_{h,i}$ のルートノードに割り当てられたラベル $LABEL_i$ からその2つの子ノードのラベルを疑似乱数生成器 G を用いて割り当てる。この処理を次は子ノードのラベルを入力として行い、孫ノードのラベルを求める。以下、同様にして部分木 $T_{h,i}$ 中の全てのノードにラベルを割り当てることができる。

【0144】

最後に、部分木 $T_{h,i}$ 中の各ノードに割り当てられたラベル $LABEL_{i,*}$ を入力として $L_{i,*} = G_M(LABEL_{i,*})$ を計算する。この値が差分集合 $S_{i,*}$ に割り当てられる暗号（復号）鍵である。

【0145】

次に、ステップS43で選択された部分木 T_h 中の部分木 $T_{h,i}$ で、ステップS44で選択されていない部分木が存在するか否かを判定する（ステップS46）。存在する場合はステップS44へ戻り、未だ選択されていない部分木 $T_{h,i}$ を選択し、同様の処理を行う。存在しない場合は、次に、 2^b 個の2分木中に存在する全ての部分木 T_h の中で、ステップS43で選択されていない部分木 T_h が存在するか否かを判定する（ステップS47）。存在する場合は、ステップS43に戻り、まだ選択されていない部分木 T_h を選択し、同様の処理を行う。一方、存在しない場合は処理を終了する。

【0146】

以上述べたように、本実施例においては、2分木を複数のレイヤに分割し、分割された各部分木に対してThe Subset Difference Methodを適用するので、記録媒体中の鍵情報量の増加を押さえつつ、再生装置の保有しておく復号鍵などの秘密情報を大幅に減少させることができる。

【0147】

また、The Subset Difference Methodにおいて、各差分集合への復号（暗号）鍵の割り当てに疑似乱数生成器を用いる場合、再生装置側で保有しているラベル情報から復号鍵を求めるのに最大 $\log_2(N) + 1$ 回の（疑似乱数生成器の出力を求めるという）演算を必要としていたが、本方式では最大 $d + 1$ 回で十分となる。なお、 d は部分木 T_h の高さである。よって、ラベル情報から復号鍵を効率的かつ迅速に得ることが可能となる。

【図面の簡単な説明】

【図1】

木構造を用いた鍵管理方式のモデルを示す図である。

【図2】

鍵管理方式により用いる木構造の例を示す図である。

【図3】

鍵管理方式により用いる木構造の例を示す図である。

【図4】

階層分割を伴う鍵管理方式の木構造の例を示す図である。

【図 5】

階層分割を伴う鍵管理方式の木構造の例を示す図である。

【図 6】

階層分割を伴う鍵管理方式の木構造の例を示す図である。

【図 7】

階層分割を伴う鍵管理方式の木構造の例を示す図である。

【図 8】

複数の鍵管理方式における記憶媒体側と受信機側の鍵情報サイズを比較するグラフである。

【図 9】

本発明の実施例に係るコンテンツ記録システムの構成を示すブロック図である。

【図 1 0】

図 9 に示すコンテンツ記録システムの各部の信号内容を示す。

【図 1 1】

図 9 に示すコンテンツ記録システムの各部の信号内容を示す。

【図 1 2】

本発明の実施例に係るコンテンツ再生システムの構成を示すブロック図である。

【図 1 3】

図 1 2 に示すコンテンツ再生システムの各部の信号内容を示す。

【図 1 4】

図 1 2 に示すコンテンツ再生システムの各部の信号内容を示す。

【図 1 5】

コンテンツ記録処理のフローチャートである。

【図 1 6】

コンテンツ記録処理における復号鍵の選択処理のフローチャートである。

【図 1 7】

コンテンツ再生処理のフローチャートである。

【図 1 8】

本発明の鍵管理方式により部分集合に鍵を割り当てる処理のフローチャートである。

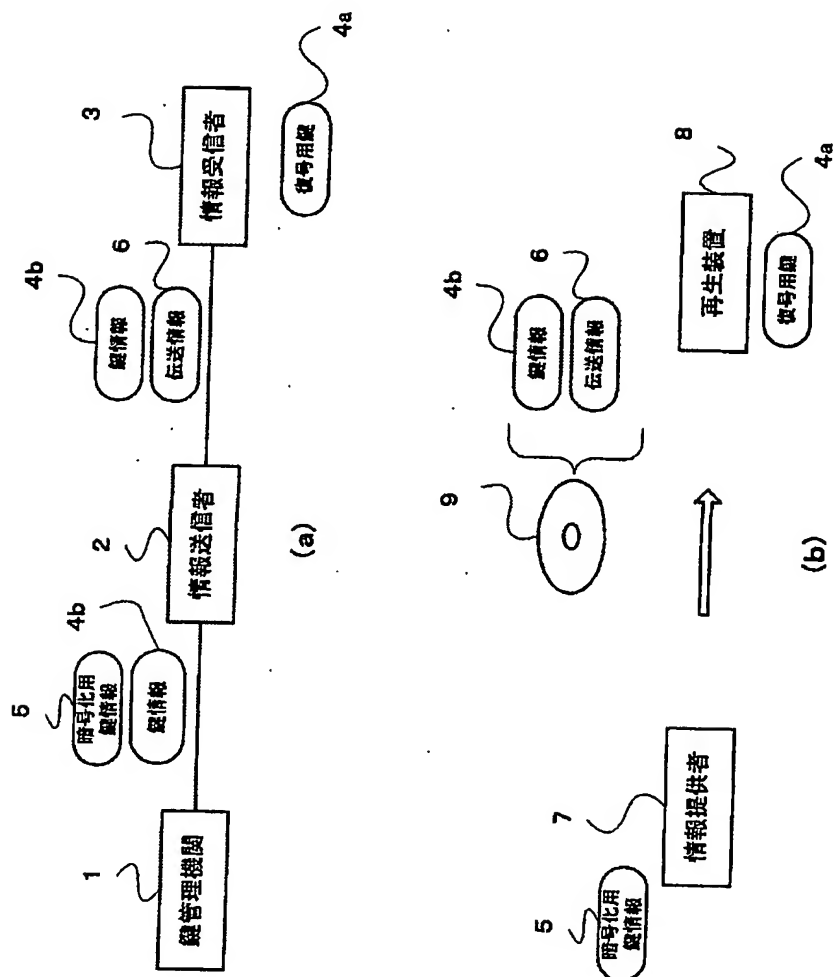
【符号の説明】

- 1 鍵管理機関
- 2 情報送信者
- 3 情報受信者
- 4 a 復号用鍵
- 4 b 鍵情報
- 5 暗号化用鍵情報
- 6 伝送情報
- 7 情報提供者
- 8 再生装置
- 9 記録媒体
- 5 0 コンテンツ記録装置
- 6 0 コンテンツ再生装置

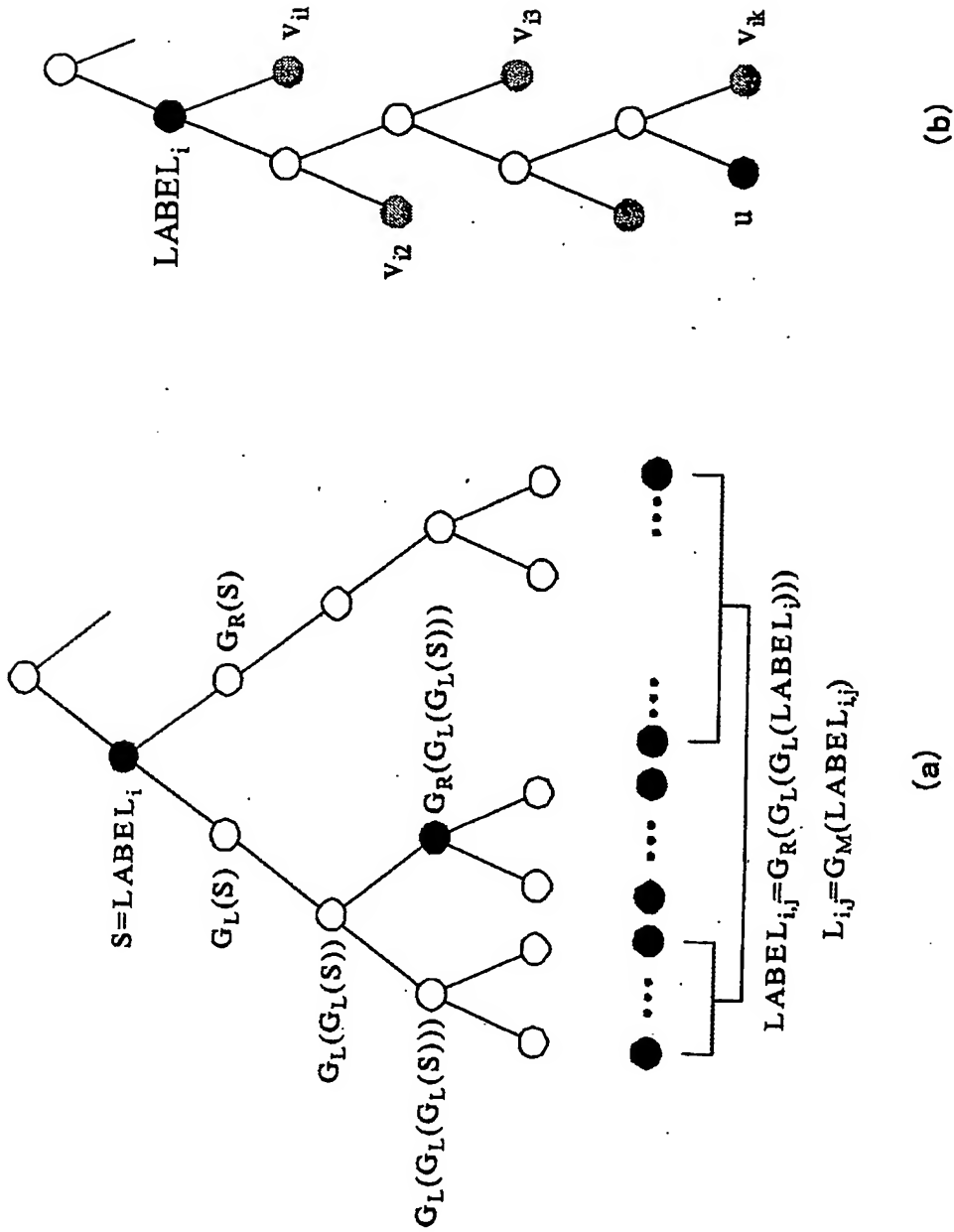
【書類名】

図面

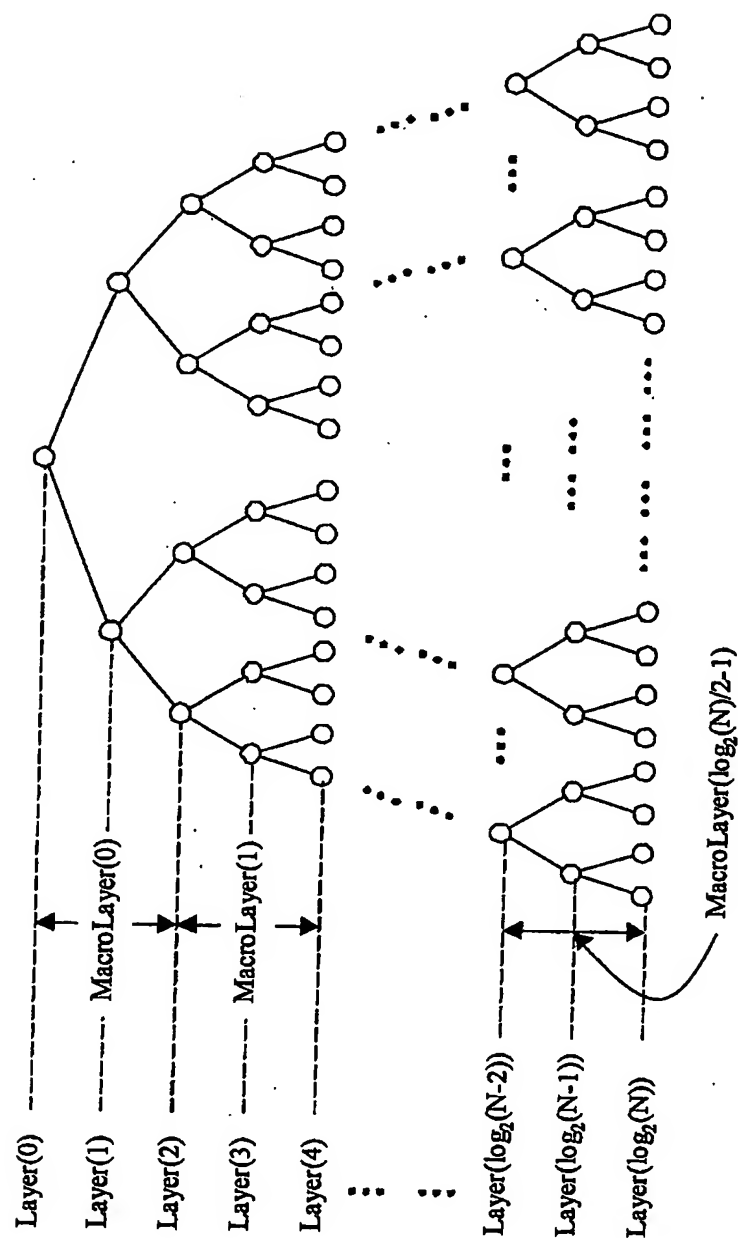
【図1】



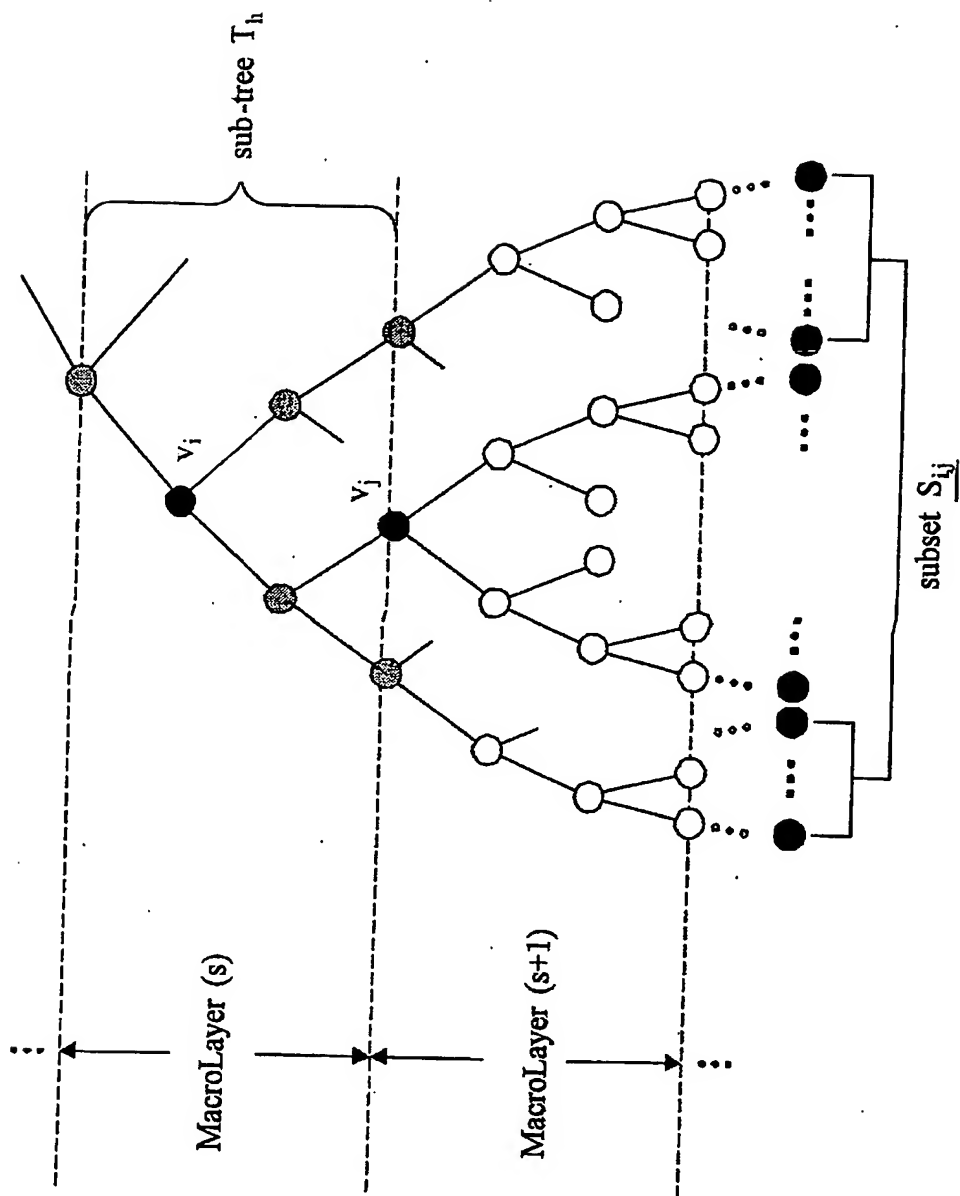
【図 3】



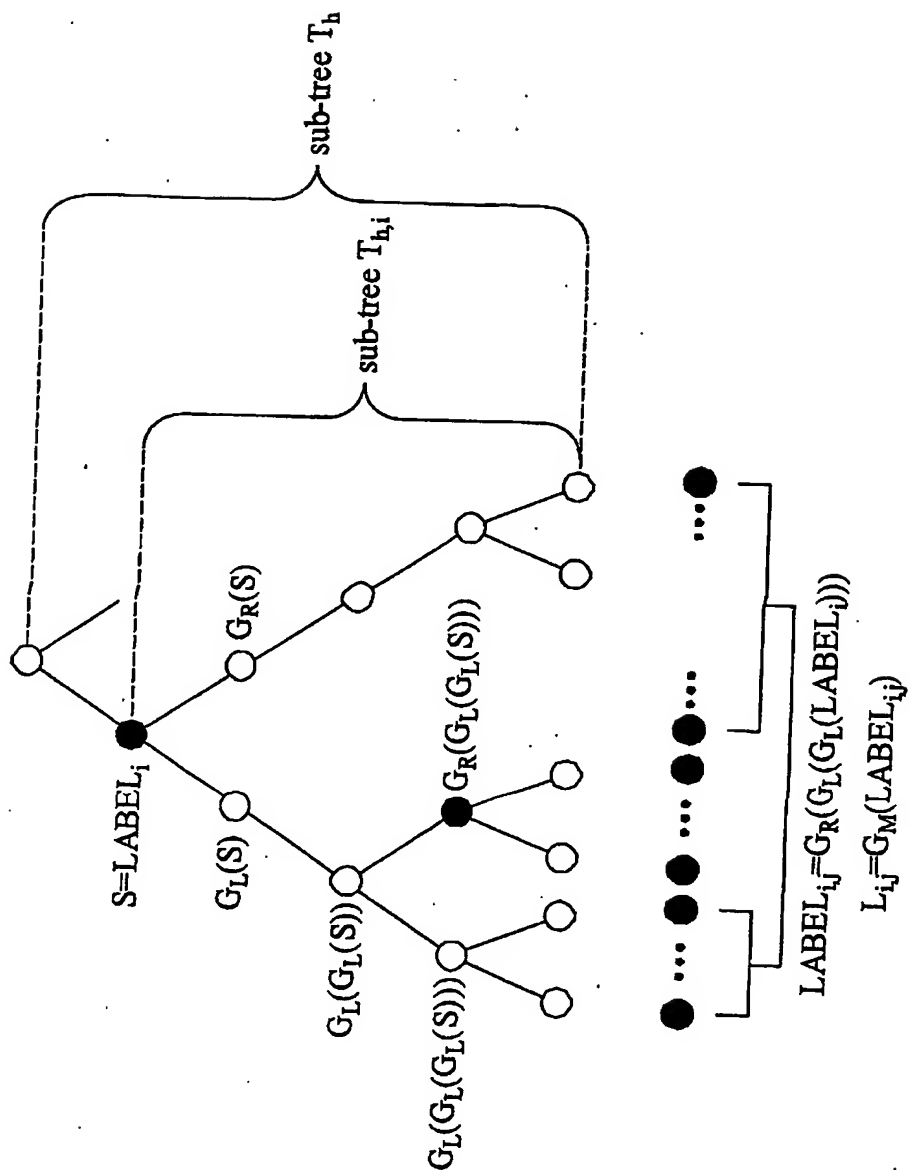
【図4】



【図 5】

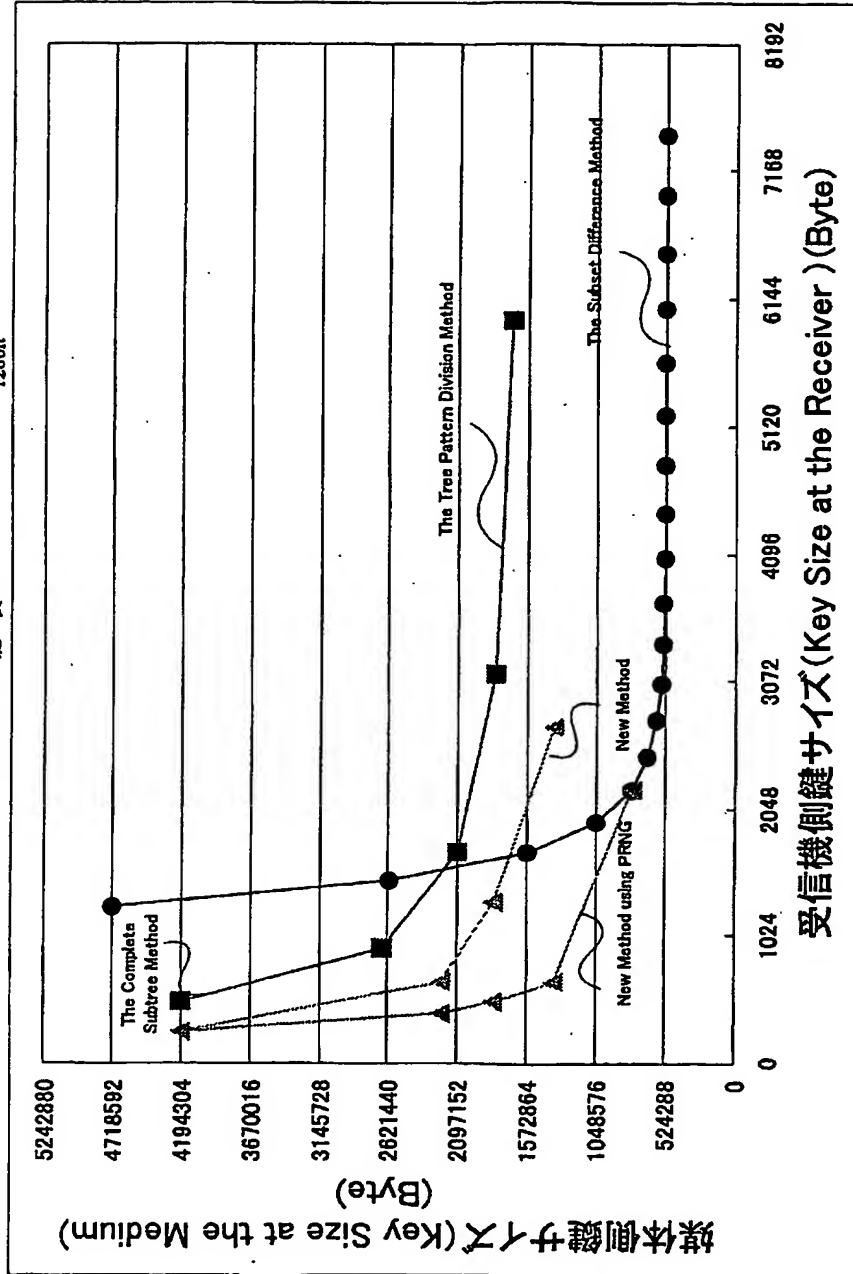


【圖 6.】

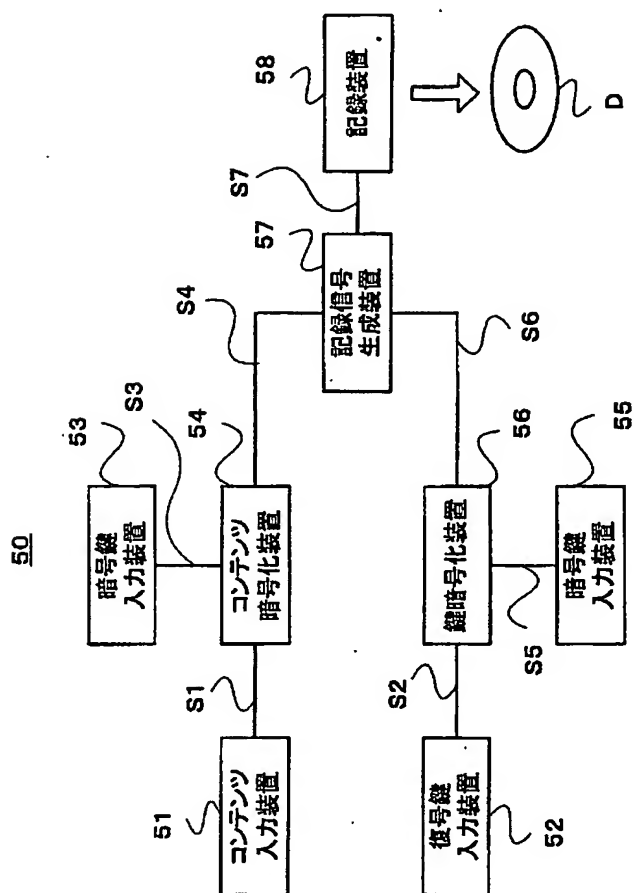


【図 8】

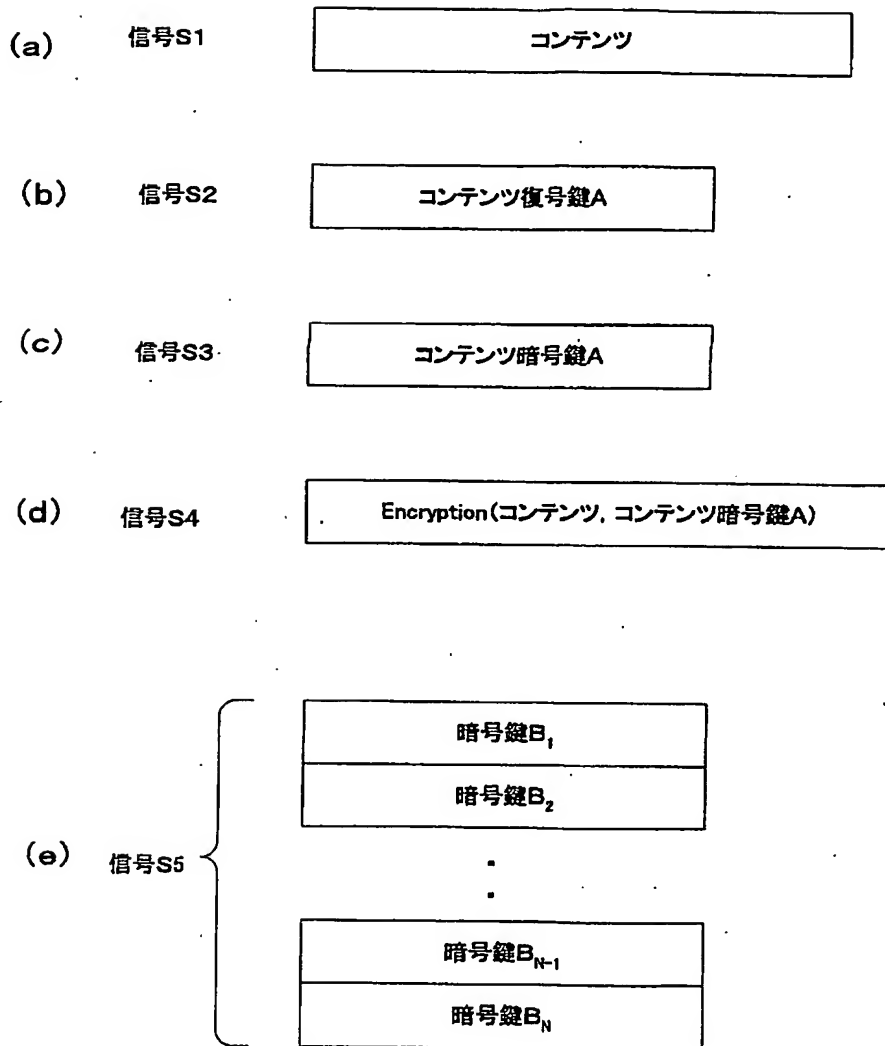
受信機総数 (The total number of receivers) $N = 2^{30} = 1,073,741,824$
 無効とする受信機数 (The number of revoked receivers) $r = 2^{14} = 16,384$
 鍵 長 128bit



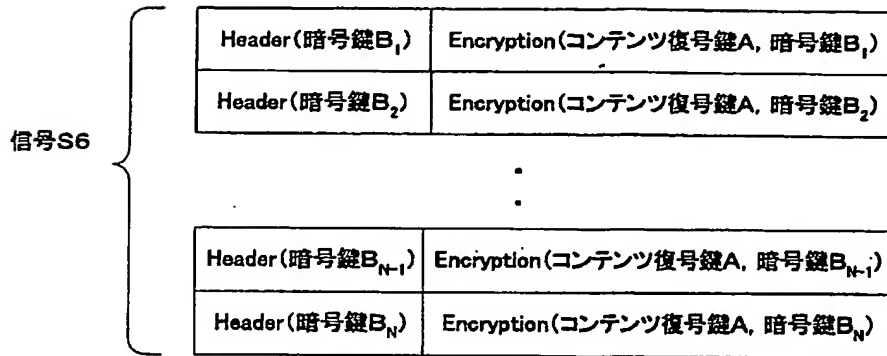
【図9】



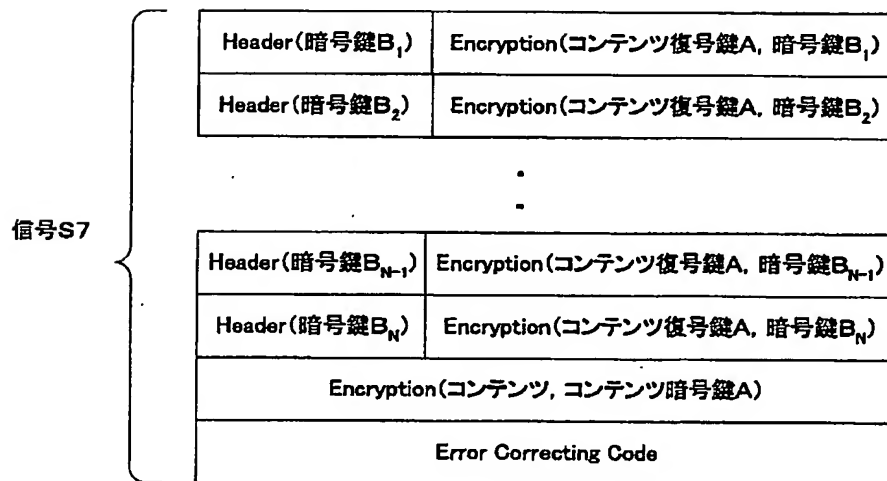
【図 10】



【図 1 1】

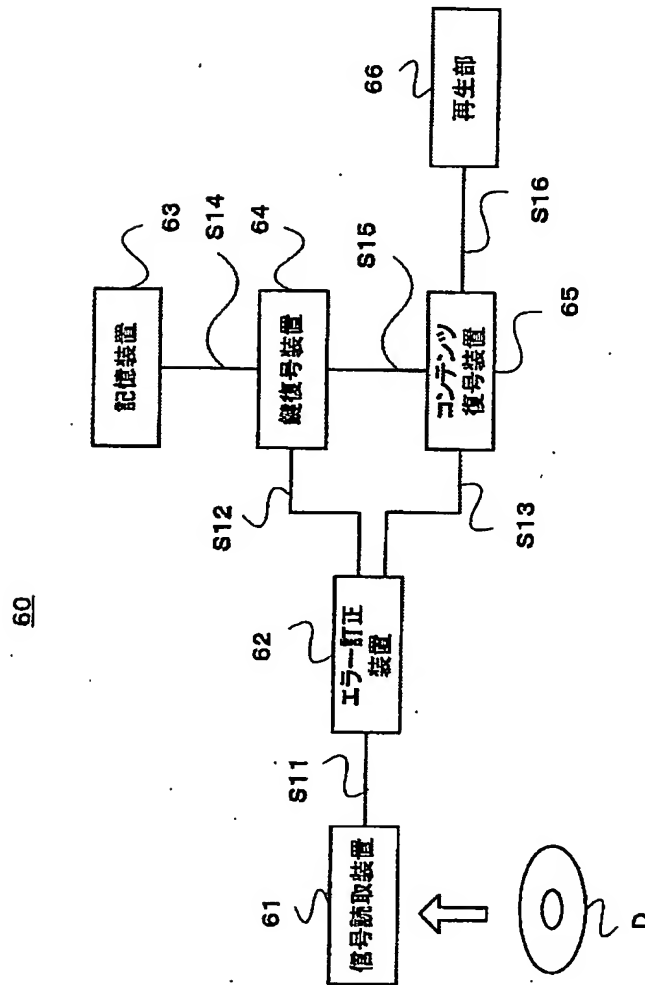


(a)

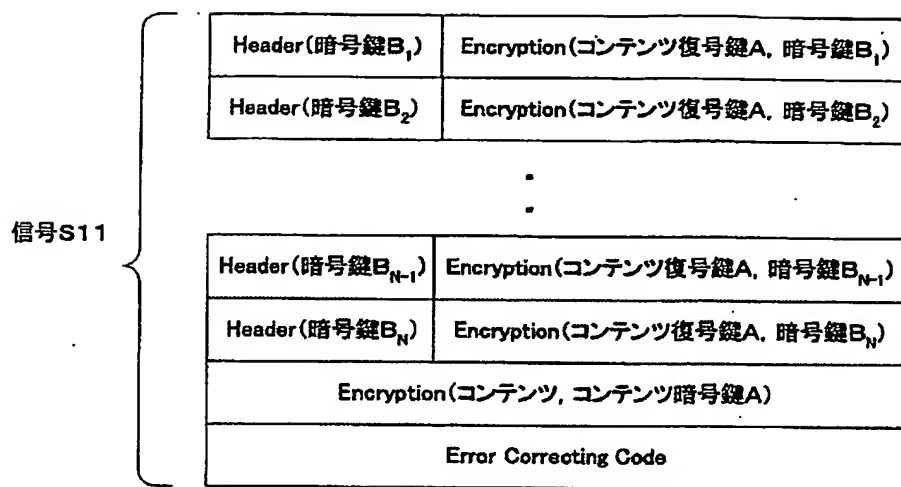


(b)

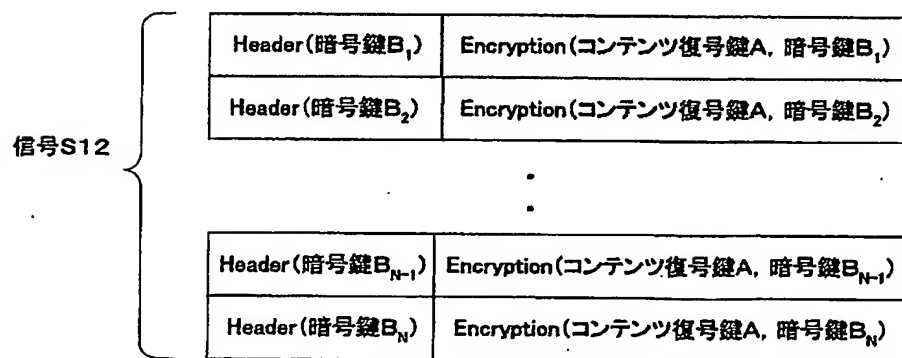
【図12】



【図 13】



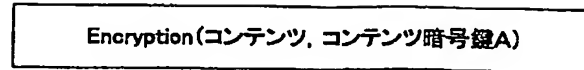
(a)



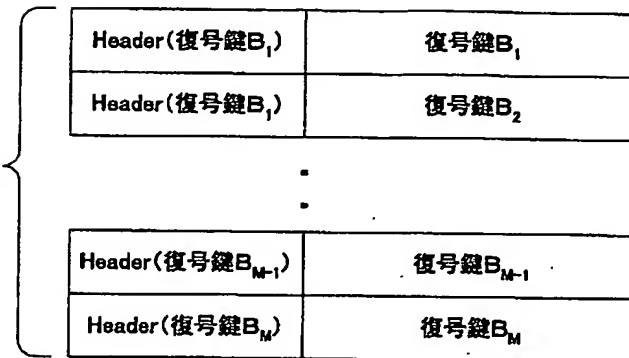
(b)

【図 14】

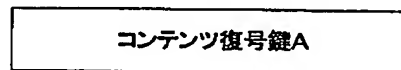
(a) 信号S13



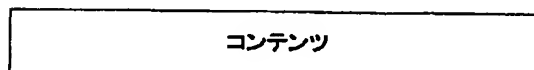
(b) 信号S14



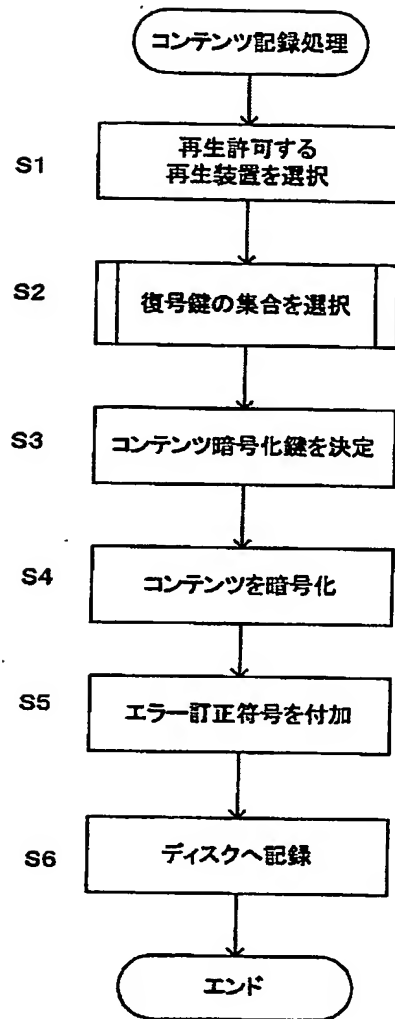
(c) 信号S15



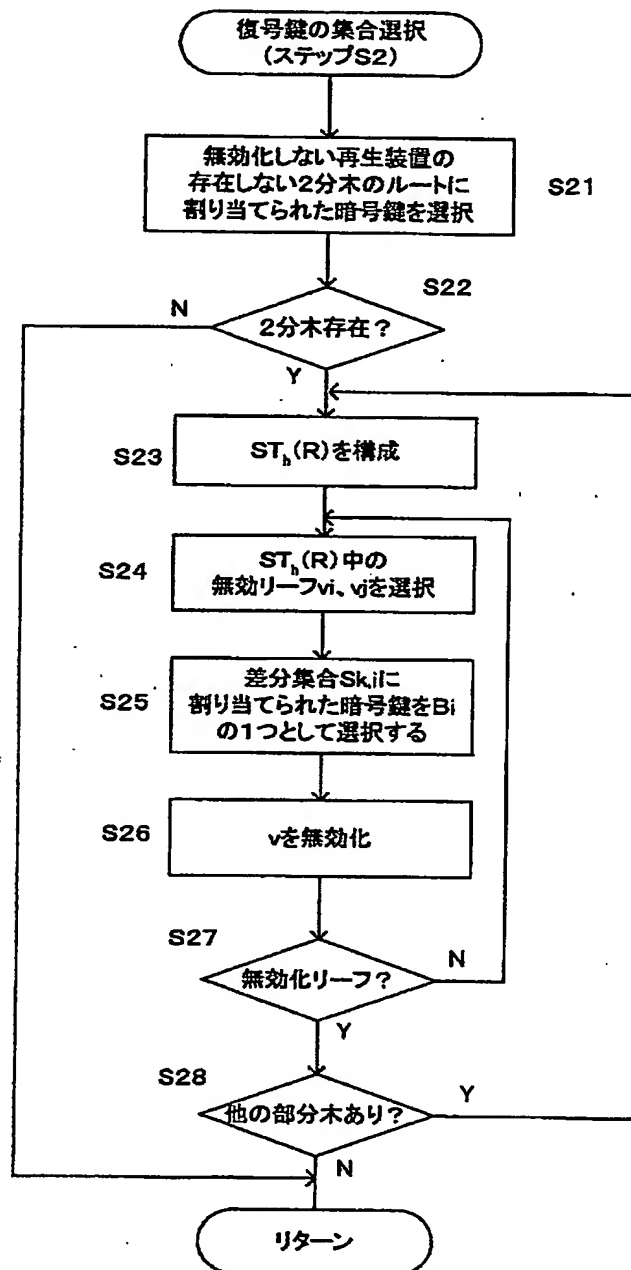
(d) 信号S16



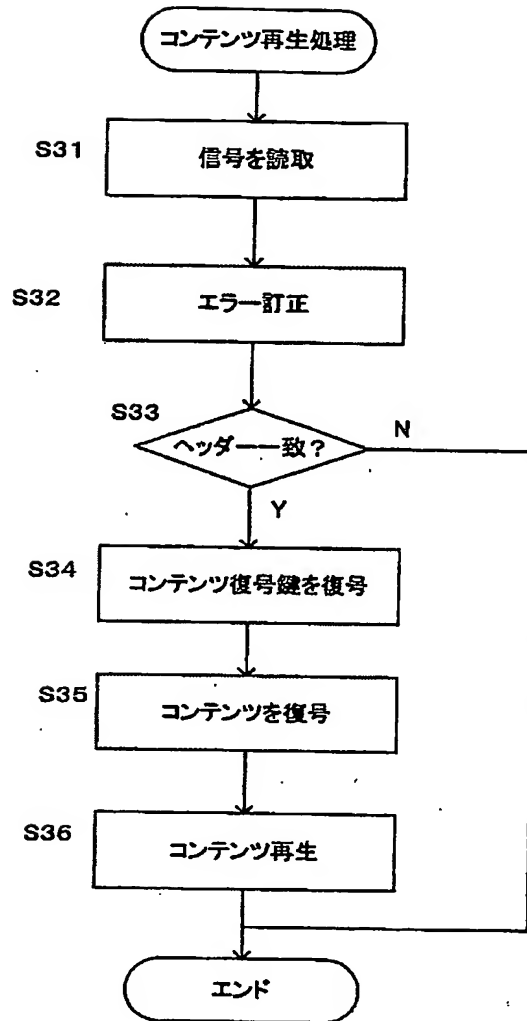
【図15】



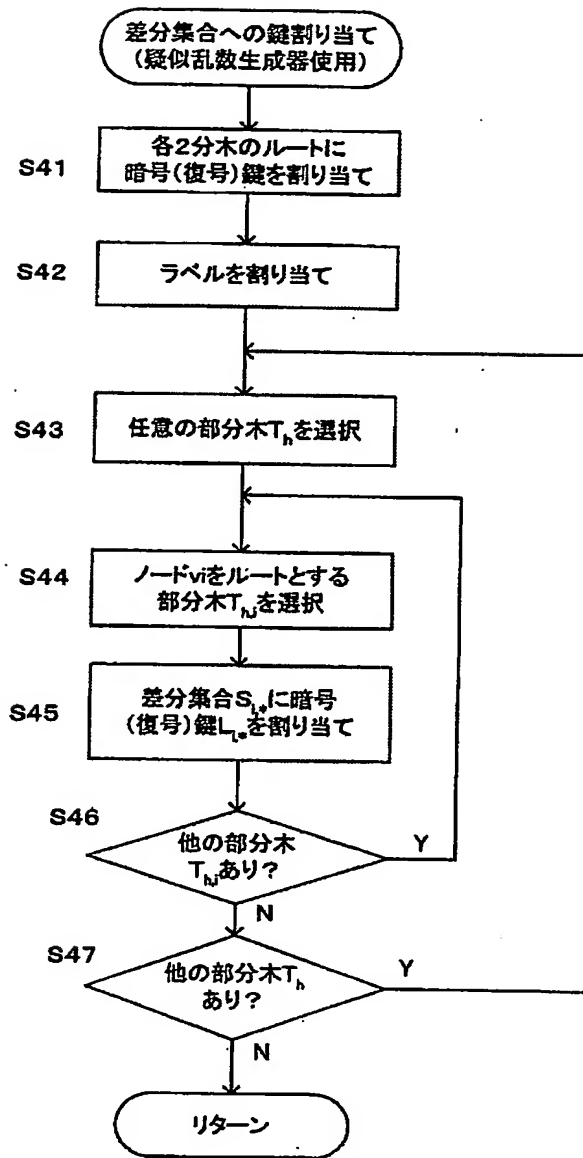
【図 16】



【図17】



【図 18】



【書類名】 要約書

【要約】

【課題】 記録媒体中の鍵情報量の増加を押さえつつ、再生装置の保有すべき秘密情報量を減少させることが可能な木構造を用いた鍵管理方式、及び、それを適用したコンテンツ記録／再生システムを提供する。

【解決手段】 情報提供者は、コンテンツを第1の暗号鍵により暗号化して暗号化コンテンツを生成するとともに、第1の暗号鍵に対応する第1の復号鍵を、第2の暗号鍵により暗号化して暗号化鍵情報を生成する。そして、暗号化コンテンツ及び暗号化鍵情報を記録媒体その他の形態で情報受信者に提供する。また、情報提供者は、予め第2の暗号鍵に対応する第2の復号鍵を生成するための情報を有しており、それを用いて第1の復号鍵を取得し、さらに第1の復号鍵を用いてコンテンツを復号化して再生することができる。第1の復号鍵及び第2の復号鍵は、情報受信者をリーフに割り当てた木構造を利用した鍵管理方式に基づいて情報受信者に配布される。ここで、上記木構造を複数の階層に分割して複数の部分木を規定し、部分木単位で鍵情報の割り当てを行うことにより、情報受信者が保有すべき鍵情報の情報量を減少させることができる。

【選択図】 図1

特2002-276306

出 願 人 履 歴 情 報

識別番号 [000005016]

1. 変更年月日 1990年 8月31日
[変更理由] 新規登録
住 所 東京都目黒区目黒1丁目4番1号
氏 名 バイオニア株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☒ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☒ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☒ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.